A Secure and Privacy-preserving Incentive Framework for Vehicular Cloud

by

Abdulrahman Alamer

A thesis
presented to the University of Ontario Institute of Technology
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Computer Science

University of Ontario Institute of Technology
Oshawa, Ontario, Canada, 2018

April 2018

I hereby declare that I am the sole author of this thesis. Any published (or unpublished) ideas and/or techniques from the work of others are fully acknowledged in accordance with the standard referencing practices.

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

Abdulrahman Alamer, 2018

Abstract

Vehicular Cloud Computing (VCC) plays a critical role in data generation where a large number of vehicles collect various kinds of sensing resources with large-volume features. The resources are diversified according to various vehicle capabilities. While the information that should be collected is essential for the success of VCC applications, how to stimulate the vehicle owners to provide their sensing resources in VCC is also crucial to its success. When vehicle owners choose to contribute their data for economically appealing compensation, they may be concerned about their privacy.

This thesis first proposes a promising secure and privacy-preserving incentive mechanism framework for VCC. An incentive to convince vehicle owners with excess on-board capabilities to join in VCC without the risk of privacy disclosure. The incentive mechanism employs game theory to model the interactions between the VCC server and vehicles. With the incentive mechanism, the VCC server, which represents the task announcement can select competent vehicles to collaborate for the announced task, and the vehicle owners can earn payments from their participation. Further, the incentive mechanism guarantees the fairness between all participants in terms of payment. This is because the critical payment scheme can ensure the truthfulness of all the participants such that each vehicle honestly reports its true sensing cost. The signcryption technique and homomorphic concept are exploited to achieve mutual authentication between the VCC server and vehicles, and prevent the privacy information of these vehicles from being disclosed. Simulation results are provided to show that the privacy-preserving incentive mechanism is beneficial to both the VCC server and vehicles to achieve a win-win situation.

Moreover, we study the situation in which the VCC server announces a spatial task that can be exploited by an adversary or malicious Roadside unit (RSU) to reveal vehicles' privacy. Protecting the privacy of participants becomes an essential to the prosperity of the VCC applications. Therefore, we propose a novel secure and privacy-preserving scheme for enhancing security in VCC-based tasks announcement. The proposed scheme combines a multiple receiver signcryption technique with proxy re-encryption in order to protect message content that includes the private information of the vehicles from being disclosed during task announcement. The scheme can achieve data confidentiality and integrity against the malicious RSU, which means that the RSU is not able to access private information or corrupt the task announcement during the recruiting process. The distinctive feature of the proposed scheme eliminates the issue of increasing the computation delay that most of the multiple receiver signcryption schemes are suffering from when the number of receivers increases. Compared to the other multiple receiver signcryption schemes, the proposed scheme is more efficient in regards to computational overhead and ciphertext size. Additionally, security analysis demonstrates that the proposed scheme is resilient against various security threats to VCCs.

In addition to the above schemes, the quality of task fulfillment strongly depends on the set of recruited vehicles. The more suitable participants are involved, the better the obtained results are. However, at the same time the more privacy is threatened for violating. Due to the fact that a VCC server is responsible for recruiting vehicles to collaborate for the announced task, the VCC server may not be fully trusted, and the disclosure of individual locations has serious privacy implications from the perspective of vehicles. It is possible for attackers to predict the trajectory and living habit of a specific vehicle. Thus, we introduce a novel framework for privacy-preserving for a location privacy-aware task recommendation framework in spatial crowdsourcing. The proposed framework enables a VCC server to recommend spatial tasks released by customers to the participants in geocast regions. By exploiting Lagrange interpolating polynomials, we design a privacy-preserving location matching mechanism, called LATE, to enable the VCC server to determine whether the interested vehicle participant is in a geocast region of a spatial task or not without having any knowledge about the task's geocast regions and the vehicle's location. In addition, the contents of spatial tasks and vehicles' reports are protected from privacy leakage for both customers and participants. The proposed scheme demonstrates the efficiency and practicality for recommending spatial tasks to suitable vehicles while protecting vehicles' privacy.

Acknowledgements

I would like to thank all the people who made this possible. This thesis would not have been possible without the help and support of my supervisors, my thesis committee members, and my colleagues in Information Forensics and Security Laboratory (IFS Lab). During my Ph.D research I learned many new things, and without the people surrounding me I could not enjoy from this period of my life.

First of all, I gratefully acknowledge my supervisor, Professor Xiaodong Lin. He made available his support and aid in a number of ways. He always does care about his students, and I had this opportunity to discuss the obstacles encountered me in my study and research openly with him. He not only helps me to develop the academic skills, but also guides me to strive for excellence.

Also, I would like to thank my co-supervisor Professor Ying Zhu for her constant support, availability and constructive suggestions, which were determinant for the accomplishment of the work presented in this thesis.

In addition, I would like to thank all the members of my examining committee, Dr. Jing Ren, Dr. Patrick Hug ,and Dr. Ramiro Liscano and Dr. Shahram Heydar, for the time and efforts to read my thesis. In spite of their busy schedules, all have been readily available for advice, reading and encouragement.

I would also like to thank Prof. Lingyu Wang as my thesis external examiner and sharing his invaluable insight on computer and communication security with me.

I would like to extend my appreciation to all the Information Forensics and Security Laboratory group for continuing support and warm working atmosphere. It is indeed a great honor to work with a great talents during my Ph.D. study at UOIT. Special thanks go to Dr. Khalid Alharbi, Dr. Aiqing Zhang, Mr. Yong Deng, Mr. Sultan Basudan, Mr. Abel Bacchus, Mr. Di Tian, Mr. Jianbing Ni, Mr. Ya tian, Ms. Yanwen Zhou for day-and-night discussion and continuous support throughout my graduate study.

Grateful acknowledgements are made for the Saudi Arabian Cultural Bureau in Ottawa for providing me with a full scholarship during my Ph.D study. I would never get this far without the support of my father, mother, sisters and brothers. I think them for always believing in me and supporting me. Their love and encouragement have been and will always be a great source of inspiration in my life. Finally, my special thanks go to my wife for the loving support and patience she has for me to fulfill my career goals.

Table of Contents

List of Tables

List of Figures

List of Acronyms

VCC	Vehicular Cloud Computing
RSU	Roadside Unit
LATE	Location Privacy-aware Task Recommendation
OBU	On-Board Unit
VaaR	Vehicle as a Resource
TPPT	Truthful Privacy Preserving Tendering
MRPRS	Multiple Receiver Proxy Re-Signcryption
WAVE	Wireless Access in Vehicular Environment
DSRC	Dedicated Short Range Communication
VANET	Vehicular Ad hoc Network
CC	Conventional Cloud
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
NaaS	Network as a Service
STaaS	Storage as a Service
CaaS	Cooperation as a Service

CompaaS	Computation as a Service
TA	Trusted Authority
GPS	Global Positioning System
WVDP	Winning Vehicle Determination Problem
TGP	Truthfulness Guarantee Problem
PPP	Privacy Preserving Problem
MPU	Memory Protection Unite
TMS	Trust Management Server
TPMSs	Tire Pressure Monitoring Sensors

Chapter 1

Introduction

1.1 Motivation

As of late, automotive manufacturers try to promote their vehicles by equipping them with a set of sensing devices, wireless communication devices and powerful On-board units (OBUs) with high computing and storage capabilities, aiming to guarantee on-road safety and to improve on-board experiences [80]. With this sophisticated equipment, vehicles can be considered as mobile resources for many services such as computing, storage and sensing [1]. Therefore, S. Abdelhamid *et al.* [2], introduced the concept of Vehicle as a Resource (VaaR), which focus on making use of various vehicular resources to generate a large number of data that can be extended to support more applications, such as vehicle fault diagnostics, vehicle noise pollution detection, and air quality forecasts.

While these vehicles can act as perfect candidates to utilize on-demand resources as services, studies show that the resources of these intelligent vehicles are not completely invested and most of these resources are wasted. In order to explore and utilize the excess vehicle's capabilities, Olariu *et al.* [59] introduced the concept of Vehicular Cloud Computing (VCC), which is an emerging paradigm that integrates Vehicle Ad-hoc Networks (VANETs) and cloud computing to provide cloud based services for the drivers. The key point of the VCC paradigm is to collect and utilize the excessive vehicles' resources in a dynamic group of vehicles under the vehicle owners' authorization. By using the vehicles' resources, the VCC becomes increasingly ideal and hence it can support many applications such as safety-related and non-safety-related applications.

It is important to know that these applications can support drivers by using mobile crowdsensing paradigms in which individuals are able to collect and contribute data using sensing and computing mobile devices (i.e., smartphones). However, mobile devices suffer from sensor limitations, which are insufficient for providing valuable data for different applications. For example, consider the following two scenarios:

- Scenario 1: Safety-related applications, which contribute to improving road safety. Notifying road surface hazards such as ice, nails, and potholes to the drivers will improve their on-road safety. Currently, most safety-related road providers rely on mobile devices such as smartphones to obtain road information. However, the data obtained from mobile device sensors are not accurate enough to estimate the road condition because of their limitations [75]. As Fig. 1.1(a) shows, if a road is suspected to have nails, mobile devices can hardly detect the existence of these potential hazards. However, using vehicular sensors can be distinguished from other mobile devices [1]. For example, once a vehicle's tire is punctured by nails, the Tire Pressure Monitoring Sensors (TPMSs) can perceive the loss of air immediately. The development of vehicle sensors that can detect road surface abnormalities and obtain real-time road information are continuously increasing. As part of the VCC system, the affected vehicle can distribute road abnormalities to all the connected vehicles and the cloud server. Thus, the hazards can be either avoided or cleared quickly, which can benefit the whole community.

- Scenario 2: Non-safety-related applications, which are used to facilitate traffic management. Providing real-time traffic information is essential for maintaining an agile traffic status by detouring vehicles away from congested roads. Knowing what is currently occurring on the roads, the drivers can decide to make their journeys much easier. Now, more and more vehicles are equipped with real-time traffic service from satellite or connected mobile devices. With real-time traffic, the drivers can choose the optimal route to avoid the delay. Also, in-car sensors can provide more accurate information compared with regular mobile devices. Here, we use Google maps as an example to show the limitations of mobile devices. As shown in Fig. 1.1(b), we can see that the road in red in Google maps indicates a traffic jam in a certain area. In fact, the jam is located in the left lane, which means that the road is only partially congested. Providing this type of inaccurate traffic information can easily mislead the drivers who intend to go straight. Nevertheless, the signal light sensor inside a vehicle can easily detect the vehicle's exact direction at an intersection. It can be seen that the data collected by a vehicle's built-in sensors is always more relevant to the road conditions.

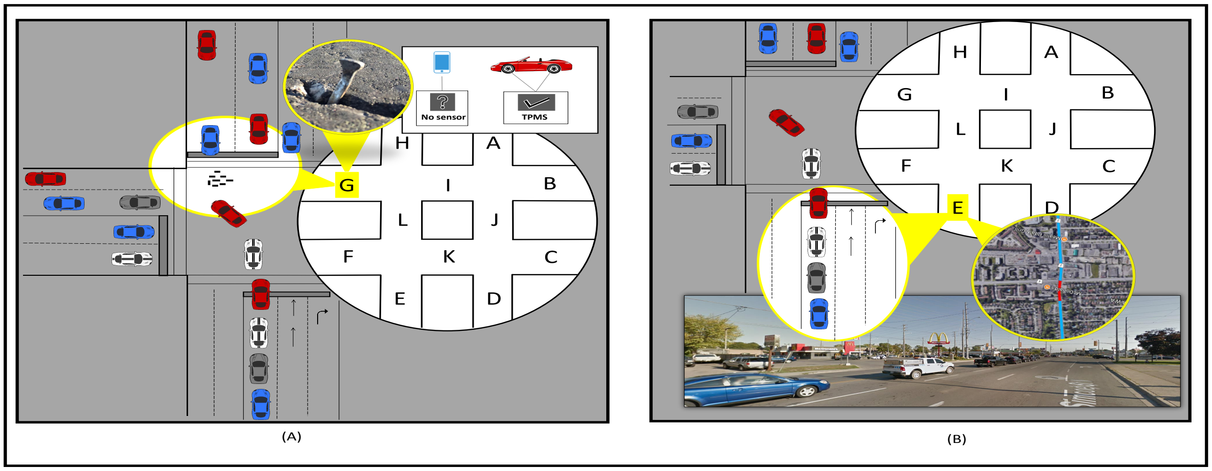

Figure 1.1: Application Scenarios of Vehicular Cloud Computing (VCC).

Thus, the VCC can benefit from the capabilities of individual vehicles and utilize them to provide more accurate and useful services compared with other mobile crowdsensing paradigms. As illustrated in Fig. 1.2, the VCC consists of three layers, the vehicles layer, communication layer and cloud layer. In the cloud layer, the customers outsource their tasks to the cloud. The cloud then releases the tasks to the Roadside unit (RSU) nodes located in the sensing areas. In the communication layer, the RSU is responsible for broadcasting the announcement tasks and returning the results to the cloud if the data requirements are met. In the vehicle layer, a number of connected in-motion vehicles cooperate with each other to achieve practical applications.

Nevertheless, adequate vehicle participation is considered a significant part of the success of VCC applications. A number of VCC applications have been proposed based on the assumption of making vehicles voluntarily contribute to the VCCs. However, there still exist several challenges that may affect the development of the VCC applications. The first challenge is whether the owners of smart vehicles are willing to participate in a VCC system. This is because when vehicles provide their resources to the VCC, they incur some costs. As a result, the vehicle owners may refuse to participate unless they receive incentives such as compensation for their resources [4]. Although the authors in [5] claim that the owner of a vehicle may intend to rent out its on-board resources with economically appealing compensation, the issue to be solved is determining how to stimulate vehicle owners to provide on-demand services in a dynamically changing environment. Furthermore, consideration must be made to determine how to select optimal vehicles and their strategies while guaranteeing fairness. The second challenge is the security and privacy-preservation issues of the involved vehicles in VCC [87]. Since the service providing vehicles are independently owned, one vehicle may not trust the messages transmitted from other vehicles unless it verifies the origin of the messages. While at the same time, the vehicle owners may be concerned about the privacy of their information disclosed such as location and identity during participation in VCC. Thus, the vehicle owners may choose not to contribute to the VCC without the protection of the private data being guaranteed. Moreover, the incentive mechanism should also protect the payment information related to the participating vehicles.

To solve the above challenges, many works have been done that use game theory, such as Stackelberg, were used to encourage vehicle owners to participate by sharing their resources in a VCC system [20] [91] [92]. However, these works did not adequately consider the problem of how to protect the privacy of the involved vehicles and how to evaluate vehicles' resources in terms of payment. For instance, these schemes provide fixed monetary rewards for each task which is not adequate to guarantee the fairness and correctness among vehicles. The vehicle that provides sensing resources will obtain the same compensation as those who provide computing or storage resources. It is important to know that the sensing resource is totally different from the computing and storage resources in terms of social cost. Vehicle owners may seek to maximize their profits by providing a different type of resources; therefore, we cannot merely compensate the vehicle that provides sensing resources the same as those who provide computing or storage resources. This encourages us to display a mechanism that is capable of evaluating vehicles' resources in an obvious way in order to guarantee the fairness and correctness between the vehicles.

Nevertheless, we still need to overcome several challenges. The first challenge is how to design a framework that is resilient to strategic users. This results in the second challenge in how carefully setting an appropriate mechanism to attract users into the VCC environment. The third challenge is how to design a lightweight privacy-preserving protocol to protect the privacy of each participating vehicle.

Therefore, the main motivation of this study is to propose a new framework for a privacy-preserving incentive mechanism in VCC. The mechanism will stimulate the vehicles to provide on-demand services in a dynamically changing environment in VCC without the risk of privacy disclosure. The proposed scheme uses game theory (i.e., auction game) as the basis of incentive mechanism to model the interactions between the VCC server and vehicles. The proposed scheme exploits cryptographic techniques such as the signcryption technique, in addition to homomorphic and bilinear pairing as the basis of the privacy-preserving scheme. Thus, the proposed scheme aids in stimulating vehicle owners while simultaneously satisfying security and privacy requirements in VCC.

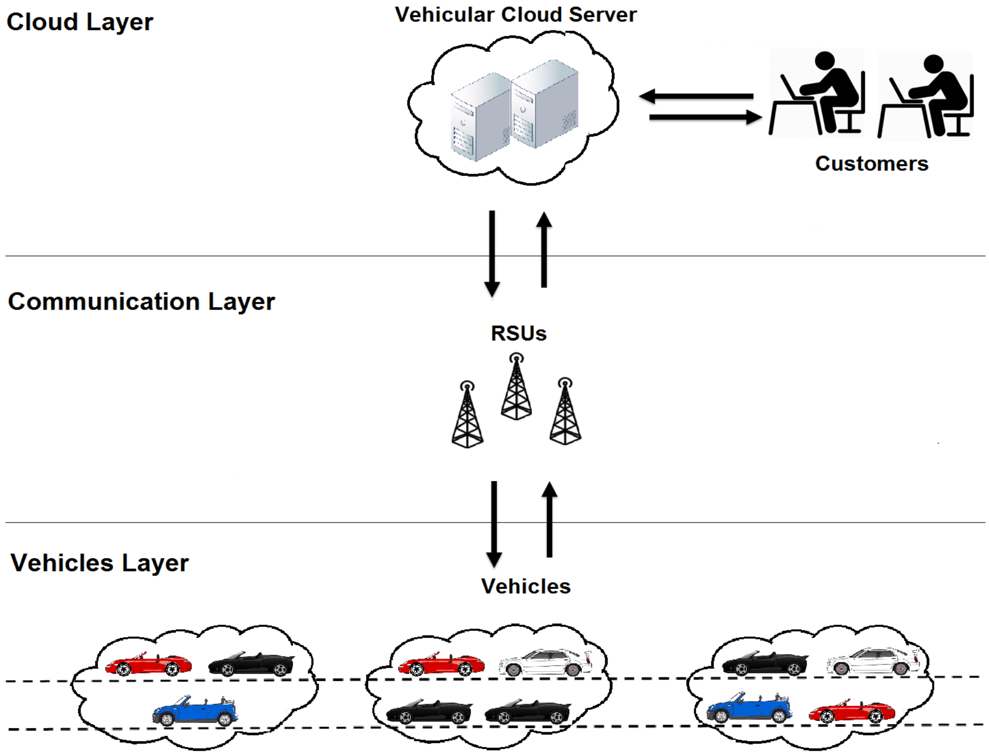

Figure 1.2: Vehicular Cloud.

1.2 Objectives and Contributions

The objective of this research is to design a secure and privacy-preserving incentive framework for VCC. This will include a privacy-preserving and truthful tendering scheme aiming to get vehicle owners to participate by pooling their collected resources in the VCC system without the risk of privacy disclosure. Furthermore, a secure and privacy-preserving task announcement scheme is proposed based on the multiple signcryption and proxy re-encryption technique in order to achieve data confidentiality and integrity for task announcements in VCC. Location privacy-aware task recommendation based on Lagrange interpolating polynomials is proposed to enable a VCC server to recommend spatial tasks released by customers to the vehicles in geocast regions without disclosing vehicles' privacy. To be more specific, the main contributions of this thesis includes:

- By exploiting game theory, a tendering-based incentive framework is proposed to stimulate vehicle owners with excess on-board capabilities to join in announced tasks in VCC. A vehicle can generate a large variety of data from the sensor devices and store them until the vehicle is selected by a VCC server as a resource provider. Based on this, we design an illustrative language that is capable of describing heterogeneous vehicular resource types as a novel approach to guarantee the fairness and correctness amongst vehicles. In addition, we introduce a *Truthful Privacy Preserving Tendering (TPPT) mechanism* that ensures truthful tenders and helps a VCC server to select the vehicle with optimal parameter for the task. The proposed framework makes use of the signcryption technique with a homomorphic concept in order to preserve the truthful information reported by vehicles from being disclosed. Compared with popular game theory schemes applied in VCC [20] [91] [92], the proposed TPPT is much more efficient and guarantees the truthful tenders. Moreover, a detailed performance analysis demonstrates that the privacy-preserving scheme is indeed significantly more efficient than the existing schemes [33] [68] in terms of both communication and computational overheads.

- By considering vehicles' location privacy may be disclosed during a task announcement, we propose a new efficient Multiple Receiver Proxy Re-Signcryption scheme (MRPRS). The proposed scheme combines signcryption and proxy re-encryption techniques. MRPRS scheme is able to eliminate the issue of increased computation delay that most multiple receiver signcryption schemes are suffering from, especially when the number of receivers becomes larger. Therefore, we use the proposed MRPRS as a concealing technique to prevent the vehicles' privacy from being disclosed during task announcements. MRPRS shows the efficiency in terms of computational costs and ciphertext size compared to existing multiple receiver signcryption schemes [83] [61] [98] and proxy re-encryption schemes in [49] [72] [45].

- The prosperity of the VCC applications are inspired by the facts that the quality of task fulfillment strongly depends on the set of recruited vehicles. However, the privacy of vehicles will be at risk of being disclosed when the VCC server recommends some of the suitable vehicles to engage in the task. Thus, we design a privacy-preserving location matching mechanism using Lagrange interpolating polynomials. The geocast region of the spatial task is encrypted using a temperate public key and a searchable tag is generated from the worker's location and the corresponding temperate secret key. Having the ciphertext and tag, anyone can test whether the worker's location is one of the places in the geocast region. By leveraging the designed privacy-preserving location mechanism, we propose a novel location privacy-aware task recommendation framework (LATE) in spatial crowdsourcing, which enables the VCC server to recommend spatial tasks released by customers to the vehicles in geocast regions. The VCC server cannot know the geocast regions of the spatial tasks and geographic locations of vehicles, but must be able to determine whether the vehicles are located in the geocast regions of spatial tasks. Therefore, the VCC server can recommend the spatial tasks to the vehicles for fulfillment. In addition, we utilize proxy re-encryption to encrypt the spatial tasks and vehicle reports to prevent privacy leakage. We prove the security of LATE to show that no attacker can learn anything about the locations of workers and the geocast areas of spatial tasks, and we demonstrate that LATE is efficient and practical in terms of computational and communication overhead.

1.3 Organization of Thesis

The rest of this thesis is organized as follows. Chapter 2 introduces an overview of vehicular cloud, architecture, security and privacy issues, applied cryptography to VCC, selfish vehicle issues, applied game theory, and related work. In chapter 3, we present a framework for privacy-preserving and truthful tendering in a vehicular cloud computing, followed by security analysis and evaluation. Chapter 4 discusses a secure and privacy-preserving task announcement scheme against malicious gateways in vehicular cloud computing and provides a security analysis and performance evaluation. Chapter 5 introduces location privacy-aware task recommendations for spatial crowdsourcing based on Lagrange interpolating polynomials. Finally, in chapter 6 will illustrate conclusions and future work.

Chapter 2

Background

2.1 An Overview of Vehicular Cloud Computing

Currently, the automotive industry is focusing on vehicular components and their relevant applications, which will classify them as intelligent vehicles. Such components include a number of sensor devices, wireless communication, and OBU for storage and operation control. With these components, a vehicle can be considered a mobile resource for many services such as sensing, storage, and computing resources. The computing resource is considered as a powerful computer, which handles computing tasks in a manner similar to a typical personal computer (PC), such as those in with dual core processors up to 2.8 GHz and storage capabilities in gigabytes [2]. Typically, storage and computing resources are tightly linked as both are provided by the OBU device that these vehicles are equipped with. Additionally, the OBU provides a broadband wireless communication that enables data transfer through 3G or 4G cellular communication systems, Wireless Access in Vehicular Environment (WAVE), Dedicated Short Range Communication (DSRC), WiFi, and WiMAX [2]. As a result, the smart vehicle, whether parked or driving on the road, forms part of a distributed system that potentially helps with management of computing tasks in an efficient and cost-effective manner in contrast to centralized systems that offer the same. In contrast, the sensing resources help to improve a vehicle performance and enhance the driving experience through monitoring its operations and the status of its parts. Where the average number of sensor devices that have been added to the vehicle can be reach to 100 sensors for supporting its operation and enhancing vehicle's services [26]. With the abundance of sensor devices, a vehicle can be considered a significant sensory resource that is impossible to be equipped with a single sensory device. For instance, plenty of resources distinguish the use of a modern vehicle as a resource from other mobile resource providers such as smartphones, which they suffer from the limited resources and lack of a trajectory prediction. Modern vehicles are considered as perfect candidates to work together with the cloud and offer a number of on-demand services.

Hence, some researchers have focused on VCC in order to utilize the extra resources of the vehicles [59] [60]. VCC is an emergent model that shifts away from the conventional VANET to a cloud service. The ultimate goals of VCC are to provide services to the vehicle drivers in real time with very little energy [29].

2.2 Vehicular Cloud Computing Architecture

Several VCC architectures have been proposed and considered by the researchers [41] [39]. Most of them have some similar components and organizations. In this chapter, we present a general VCC system architecture.

2.2.1 VCC system architecture

A typical VCC framework extends the traditional cloud infrastructure concept by integrating a VANET communication to provide services with real time information. It is mainly composed of vehicles, RSUs and a cloud server.

- Vehicle: Most vehicles are smart vehicles that equip themselves with various sensors, a powerful OBU along with communication capabilities. Consequently, the vehicles are able to collect all kinds of data from onboard sensors, and share them with the connected vehicles or the cloud server.

- RSU: The RSU usually acts as a stationary member, which is a bridge between the vehicles and cloud server. Even without sufficient computing power, it can still make the communication between the vehicles and cloud server much easier and trustful.

- Cloud server: The cloud server is a control center with powerful computational and storage capabilities. It constitutes of a cloud infrastructure layer, cloud service layer and cloud applications layer [39]. The cloud infrastructure layer contains the cloud storage and computation. This layer is responsible for aggregating computation, and vehicular storage as well as the data that are involved in VCC. Generally, the cloud infrastructure layer sends the aggregating resources to the cloud service layer and cloud applications layer for multiple services.

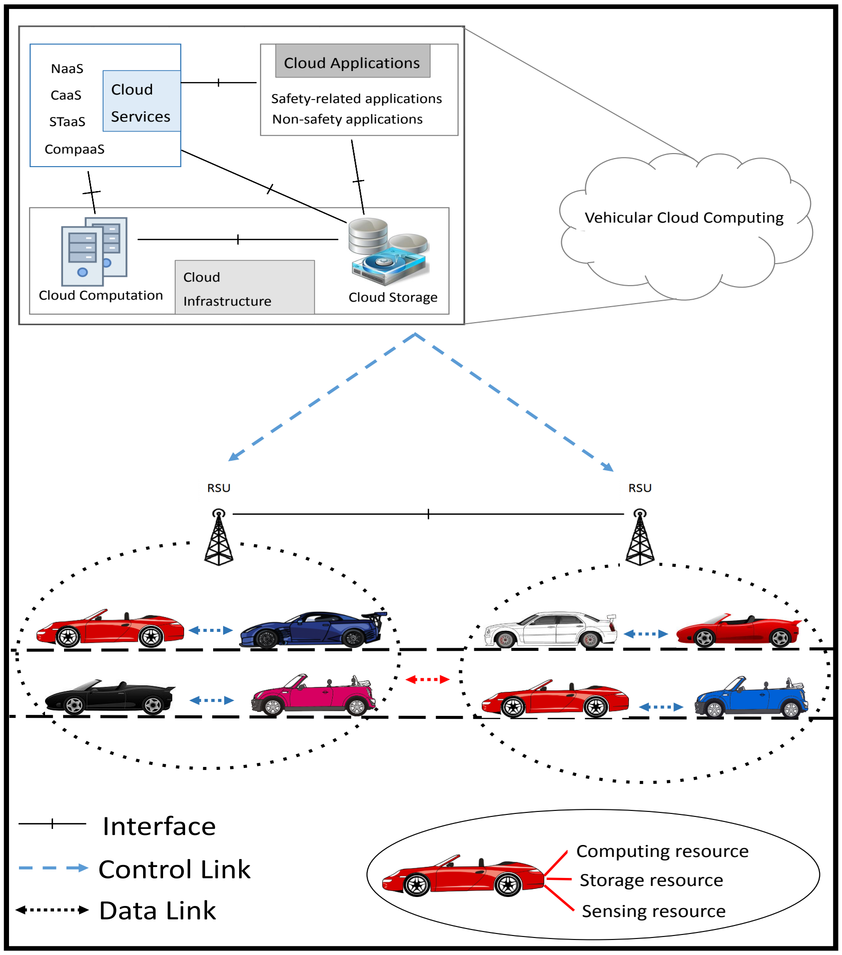

Figure 2.1: Vehicle Cloud Architecture.

As illustrated in Fig. 2.1, a cloud server, RSU nodes, and smart vehicles cooperate with each other within the VCC system. The vehicles collect various information periodically or incidentally from their onboard sensors during moving. The cloud server recruits vehicles to fulfill some tasks with the data they collected along the road. Vehicles also connect with each other by different communication modules that form a large vehicular network. In this network, vehicles with high activity level means a large amount of communications, which in turn have more chances to be recruited as a task execution entity by the cloud server. During the process, the RSU helps make the data transmission smoother between the cloud server and vehicles. Based on the task, vehicles send the related data to the cloud server via the RSU over wireless connections [39]. Apart from the vehicle-server communication, vehicles could also choose to request the data they need from the connected vehicles through connection such as V2V communication [48].

2.3 Vehicular Cloud Computing Security and Privacy

The main purpose of developing VCC is to provide more information on road conditions with the promise of making roads safer for vehicle drivers. However, to adopt the VCC system more widely, we need to address several challenges in the real VCC applications. Amongst the top challenges are security and privacy issues of the involved vehicles in VCC [87] [90]. This is because in the VCC system, the authorized users as well as adversaries are located within the same infrastructure and end up sharing the same privileges. Thus, when the data is uploaded to the VCC server, the participating vehicles lose control over their collected data. Subsequently, the adversaries can break into the system to further their malicious intentions, including access to the confidential data or may even attempt to interfere with the integrity of data. Where the forged reports may directly impact the results, and further mislead customers to make irrational decisions. As a result, one vehicle may not trust the message transmitted from other vehicles in a VCC environment, unless it verifies the origins of the message. In addition, to build successful VCC applications, the VCC server should recruit a large number of vehicles to participate in announcement tasks. However, the vehicle owners may be concerned about the privacy of their information disclosed such as their locations and identities during participation in VCC. As a result, the vehicle owners may refrain from participating to the VCC without obtaining a guarantee for protecting their private data. Therefore, security is essential to the prosperity of the VCC applications. Only a healthy and secure VCC environment can bring individuals more benefits and attract more individuals to participate in VCC applications. The basic security requirements for VCC related services include integrity, data confidentiality, authentication and protection of privacy. These are discussed in a detail.

- **Confidentiality**: In VCC, the adversary or malicious RSU can easily reveal the sensitive information from the message reports. Although the RSU is considered to be honest, it is interested in the reports generated by vehicles. Therefore, consider the data that is generated by vehicles and which is forwarded to the VCC server via RSUs as facing the attack of revealing the source of private information. For example, when a vehicle sends a road event report to a cloud server, it may include some private information about the vehicle. The malicious RSU can eavesdrop on all the data passed through it to the cloud server and discloses the confidentiality of a message that may include a vehicle's sensitive information. Furthermore, the malicious RSU can infer secret information from the intersection of multiple message reports such as the trajectory of a specific vehicle. Thus, the confidentiality of vehicle's reports is the primary objective to achieve. Data encryption can be used to protect the sensitive information against curious attackers.

- **Authentication and Integrity**: Authentication and integrity are another critical aspect related to the functionality of vehicles' reports. If the vehicles' reports are delivered by an untrusted vehicle or compromised by a forged attack and send it to the VCC server, it could lead to severe damages that cannot be recovered such as accidents or financial damages. For example, although a vehicle is considered as an honest user to submit reports for benefits, the malicious vehicle or RSU can modify any accident report message before forwarding it to the VCC server in order to trick the VCC server into accepting false results. As a result, when insurance companies seek accident reports, they may not be able to reach the driver that caused the accident. Therefore, it is worthwhile to ensure that the source of vehicles' reports are fully trusted and behave honestly. In order to successfully defend against forged data attacks, authentication and integrity should be guaranteed in any vehicle's report such as digital signatures and only the original messages from legal members should be accepted.

- **Privacy Protection**: Identification and localization of vehicles are also a major challenge to the privacy protection in the VCC system [89]. Due to the fact that multiple VCC applications require a vehicle's location and identity, they can be easily disclosed by an eavesdropper. The message that is sent by a vehicle to the VCC server devoid of content oriented privacy may result for disclosing private information of the vehicle. For instance, reporting sensing data from the surrounding environment may relate to some aspects of the drivers or even passengers and their social setting. For example, where drivers are located, heading, visit frequently, or which activity they prefer to do in vehicles. Thus, in order to protect vehicle's privacy, cryptography should be applied to important information.

2.4 Applied Cryptography to Vehicular Cloud

This section gives a brief overview of different common cryptography methods that are widely used in many standards, technologies and academic works recommended for the VCC paradigm. Superficially, the security and privacy issues in VCCs may look similar to those experienced in other networks. However, the characteristic features of VCCs introduce many of the classic security and privacy challenges. For example, the high mobility of vehicles is liable to cause significant challenges in terms of managing authentication and protecting vehicles' privacy during transmission data in VCC. In this thesis, we take advantage of some specific cryptographic techniques to ensure that the vehicle's privacy and the transmitted data in a VCC system are secure. In the following subsections, we will introduce the basic concepts of some cryptographic techniques used in this study and they will be examined in more detail, several chapters later.

2.4.1 Symmetric and Asymmetric Cryptosystems

Cryptographic systems are operations employed to transform a plaintext to a ciphertext. It is the processing method of the input data and the number of keys [77]. For instance, when the same key is used to encrypt and decrypt the message, it is called symmetric cryptography and when different keys are deployed for encryption and decryption it is referred to as a public key or asymmetric cryptosystem. The advantages and disadvantages of each of these cryptosystems are well studied in [53] and their key length, hash function, digital signature and computational performance are compared with each other. In the VCC system, asymmetric and symmetric encryption methods have not widely been used in the literature.

In this work, we adopt symmetric and asymmetric cryptosystem techniques to design a secure and privacy-preserving scheme with a variety of security purposes.

2.4.2 Signcryption Technique

A traditional approach to guarantee the confidentiality and integrity for each message is to digitally sign a message followed by a public key encryption. This approach is referred to as a sign-then-encrypt scheme. The cost involved in this approach is the sum of the cost involved by signing the message added to the cost of encrypting it. The sender would sign the message using an already chosen digital signature scheme and then encrypt the message using a public key encryption scheme separately. One of the main disadvantages of the aforementioned algorithm is that when the message is signed and then encrypted some extra bits are appended to the transmitted data which causes more machine cycles. In addition, the computational complexity to decrypt the received message is increased which in turn leads to higher costs of transferring data using this approach [101].

Therefore, to tackle this problem, a new cryptographic concept termed signcryption was first introduced by Zheng [101], which is considered as a promising paradigm in the public key cryptography. In the signcryption technique both the digital signature and encryption are performed concurrently in one step. Although the signcryption technique performs the signature and encryption simultaneously, the computational costs and communication overhead are much lower compared to the aforementioned algorithm [7]. Due to these advantages, several signcryption schemes were proposed [93] [34] [33] [68].

2.4.3 Proxy Re-encryption Technique

A proxy re-encryption is a technique in which a proxy converts an encryption message under Bob's public-key into an encryption message purposed to Chris. The main concept of this technique is to allow Bob to reveal the contents of a message sent to him and encrypted with his public key to Chris, without disclosing his private key to Chris, as shown in Fig. 2.2.

On the other hand, the proxy can convert an encryption message without knowing the secret keys of Bob or Chris and does not learn the plaintext during the conversion [6]. The framework of a proxy re-encryption technique is defined as the following:

- Key Generation. Let $\mathbb{G}$ be a multiplicative cyclic group of order q, and g be a generator of $\mathbb{G}$. Bob randomly chooses $x_b \in Z_q^*$ as his private key sk_b and computes his public key as $pk_b = g^{x_b}$. Similarly, Chris's private key sk_c is $x_c \in Z_q^*$ and the public key is $pk_c = g^{x_c}$.

- Encryption. The sender (Bob), selects $r \in Z_q^*$ randomly and encrypts the message m using his public key pk_b and delegates Chris to decrypt the message as in the following formulas:

  - $C_B = Encrypt(pk_b, m)$.
  - $Rkey_{B \to C} = (sk_b, pk_c)$.

  Then, Bob sends the $Rkey_{B \to C}, C_B$ to the proxy.

- Proxy Re-encryption. When the proxy receives the encrypted message from Bob that intends to Chris, it will re-encrypt the message using the $Rkey_{B \to C}$ as in the following formula:

  - $C_c = Re - encrypt(Rkey_{B \to C}, C_B)$.

  Then, the proxy sends the C_c to Chris.

- Decryption. The receiver (Chris) uses his private key sk_c to decrypt the ciphertext as in the following formula:

  - $m = decrypt(sk_c, C_c)$.

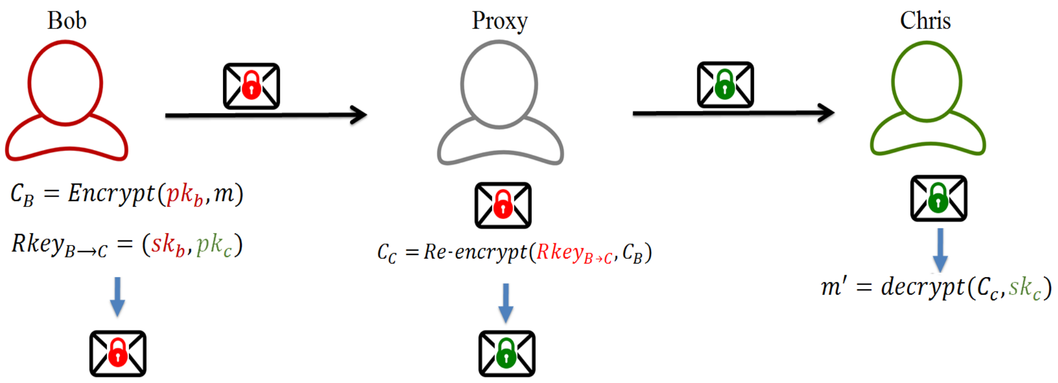
Bob
Proxy
Chris
$C_B = Encrypt(pk_b, m)$
$Rkey_{B \to C} = (sk_b, pk_c)$
$C_C = Re\text{-}encrypt(Rkey_{B \to C}, C_B)$
$m' = decrypt(C_c, sk_c)$

Figure 2.2: Proxy Re-encryption Process.

2.4.4 Homomorphic Encryption Technique

The homomorphic encryption technique has a unique feature that allows arithmetic computations to be carried out on an encrypted message to produce a new encrypted result, which when decrypted, the result will give the same result when doing arithmetic on a plaintext [58]. Moreover, the homomorphic encryption technique can be used to facilitate the analysis and detecting of the replicated data among the encrypted messages. For example, given n encrypted vehicles' bidding values $(b_1, ..., b_n)$, we can find a set of users that has the same report values while they are encrypted.

These cryptography techniques that are discussed above are important to the current research. In this work, we combine the signcryption technique and proxy re-encryption as well as a homomorphic concept to achieve an efficient privacy-preserving scheme in order to protect vehicles' privacy from being disclosed.

2.5 Selfish Vehicle

Vehicles are considered as a perfect candidate to provide on-demand resources as services. Hence, a number of VCC applications have been proposed, which are based on the assumption that vehicles voluntarily contribute to the VCC. However, the participating vehicles may incur some cost when they provide their resources to the VCC (e.g., bandwidth, storage, computing and battery of vehicles and sacrifice partial privacy about drivers). As a result, the vehicle owners may stop their participation until they obtain some incentives and compensation for their resources [5]. These type of vehicles are called selfish nodes. The selfish nodes may create challenges in development of the real VCC applications. The first challenge may result in the question of how to stimulate vehicle owners to provide on-demand services in VCCs. The second challenge is how to select the suitable vehicles with guaranteeing fairness. Thus, a well-designed incentive mechanism that stimulates vehicles to participate with ensuring the fairness amongst them is quite important.

In VANET, selfish nodes have received vast attention with incentive mechanisms being proposed as the most viable way of keeping such selfish nodes to a minimum by encouraging contribution [14] [16] [44]. It is important to note that although the schemes are beneficial to VANETs, they are unsuitable to the VCC system. The basic motivation behind stimulation in VANETs is to encourage vehicles to route and broadcast traffic related messages, which is fundamentally different from VCC. In this chapter, we will review some of the incentive mechanisms proposed for minimizing selfish vehicles in the VCC that are related to our work.

2.6 Applied Game Theory to Vehicular Cloud

Game theory plays a critical role in modeling the interactions between groups of people. There are two main branches of game theory: cooperative and non-cooperative game theory. Cooperative game theory deals with groups of people as the unit of analysis, which requires a cooperation among themselves to achieve certain goals. Non-cooperative game theory deals with how rational individuals interact with one another in an effort to achieve their own goals. This type of game theory is all about decision making within strategic settings. The user needs to consider both preferences and rationality of others users in their decision to create the best outcome for himself [30]. Thus, non-cooperative game theory is described by its players and a strategy profile for each player. In this regard, a strategy profile is defined as a set of strategies for an individual player that holistically specifies all gaming actions. In non-cooperative game theory, one player's decision may affect another player's payoff and hence every player tries to find the optimal strategy (Nash Equilibrium) to maximize his payoff. The Nash Equilibrium [54] is a term used to describe an equilibrium where each player's strategy is an optimal response to the anticipated rational strategy of the other player(s). No player is able to improve their payoff through alteration of its strategy. Based on this concept, many game theories exist such as Stackelberg equilibrium [76].

Central to game theory's application is the incentive mechanism, which is defined as something that triggers a particular course of action. The incentive mechanisms are important in interactions that focus on the motivation of players to improve profitability and productivity, and reduce absenteeism [36] [37] [50] [65]. For instance, consider two firms as a leader and a number of followers sharing bilateral interaction. When the leader offers an incentive for meeting a specific goal, the followers are likely competing between each other and every follower tries to find his best strategic action (Nash Equilibrium). The leader then selects one or a set of followers with optimal strategies as winners to achieve their goal. The incentive will be given to the winning followers as a reward when the goal is met. The leader firm uses rewards as incentives to stimulate desired behavior. Therefore, the incentive is a useful mechanism to induce a positive attitude and motivate follower firms.

Due to the fact that vehicles are selfish and rational, which they are interested in maximizing their profits, we refer to them as a non-cooperative game theory. Therefore, in this thesis, we take advantage of some specific game theory models to design incentive mechanisms between the VCC server and vehicles. While given the right incentives, vehicles may have the motivation to contribute their under-utilized resources in VCC. Thus, both the VCC server and follower vehicles can benefit from the task, and a win-win situation can be achieved. In the following subsections, we will introduce some game theory techniques used in this study and they will be examined in more detail in the following chapter.

2.6.1 Stackelberg Game Model

The Stackelberg model is considered a sequential game [78], where there are two firms that offer homogeneous products and compete by choosing the quantity of output Q_1 and Q_2 to produce. The firms are considered the leader and follower firms, where the leader has the power to decide first the quantity of Q_1 to sell and the follower firms can observe what the leader has decided for Q_1, and choose Q_2 accordingly to maximize their profits. Leader firm always knows how the follower firms will react to its decision. Thus, the equilibrium is reached when the leader and the follower firms are aiming to maximize their profits. The leader firm moves first and produces a large output of Q_1, while the follower firms are forced to produce less output of Q_2 [30].

2.6.2 Auction Game Model

In an auction system, the auctioneer announces the price for the object as long as two or more bidders are willing to participate. The auction system will stop when there is only one bidder giving a price that is higher than the other bidders. The design and analysis of auction systems are one of the triumphs of game theory. This is because game theory has a strong mathematical foundation that make it an essential tool for modeling and designing automated decision-making processes in interactive environments. For example, one might like to design efficient bidding rules for an auction website, or negotiation rules for purchasing communication bandwidth. The first auction game theory was introduced by the economist William Vickrey in 1961 and practically used in the 1990s when auctions of radio frequency spectrum for mobile telecommunication raised billions of dollars [35]. Afterward, many principles for sound bidding can be illustrated by applying game-theoretic ideas to simple examples.

In this work, we study the incentive game theory in terms of task types and vehicles' resources. Therefore, we introduce a reverse auction system in VCC, which is known as a tendering system. Where a tenderee presents an assignment as long as two or more tenderers are willing to participate. The tenderers will then submit their tenders cost to the tenderee. The tenderee will select the tenderer who has a lower cost amongst them and stop the tendering system. Thus, both the VCC server and follower vehicles can benefit from the task, and a win-win situation can be achieved.

2.7 Related Work

Many works have been done to address the challenges arising out of security and privacy requirements, and selfish vehicle issues in VCCs. In this section, we will briefly review some of the most recent privacy-preserving incentive mechanisms introduced in the literature about VCC and some existing cryptographic approaches that are related to our work.

2.7.1 Security and Privacy-preserving Incentive Mechanism in Vehicular Cloud

Recently, a lot of attention has been directed towards VCC [22] [60]. In VCC, a vast number of spare intelligent vehicles are viewed as service providers with plentiful onboard resources, which are capable of providing various services. However, not all vehicle owners are willing to provide their under-utilized onboard resources and participate in VCC. These type of vehicles are referred to as selfish nodes. Selfish nodes have received vast attention with incentive mechanisms as the most viable way of keeping them minimal by encouraging contribution.

Thus, L. Duan *et al.* [20] proposed a reward-based collaboration mechanism, where the client first determines a total reward, and then announces it among collaborators. The client should know the user's collaboration costs in order to choose only users with the lowest costs by offering a small total reward. If the client does not know users' private cost information, then he needs to offer a larger total reward to attract enough collaborators.

D. Yang *et al.* [91] [92] designed incentive mechanisms for vehicular sensing, where they consider two system models; the platform-centric model that is responsible for providing a reward shared by participating users, and the user-centric model who has more control over the payment. They used a Stackelberg game as an incentive mechanism, where the platform is the leader and the users are the followers.

However, these works still did not consider the problem of how to preserve the privacy of the involved vehicles. Consideration must be made to determine how to provide fair incentives to encourage vehicles to participate in a VCC system without the risk of privacy disclosure.

Lee *et al.* [40] proposed a secure incentive framework, which encourages cooperation among vehicular users in a secure way by leveraging a public key infrastructure to provide secure incentives for cooperative nodes. The authors in [95] studied a game-theoretical resource allocation strategy with a virtual machine migration in a cloud-based vehicular network. Lim *et al.* [46] proposed a scheme to protect the privacy of vehicles while contributing their resources for services in vehicular cloud-based on secure token reward systems.

Zhou *et al.* [103] proposed a threshold credit-based incentive mechanism to motivate cooperation among intermediate nodes, which maximizes the interest of vehicles, and guarantees the fairness for participation in the vehicular cloud. In contrast, the authors in [47] proposed a secure architecture for the vehicular cloud to encourage the potential vehicles to contribute their excess resources to the cloud by issuing them secure tokens.

However, these incentive models require the real cost of vehicular resources to be known to the cloud server, which is not practical. This is because the real cost information is considered part of vehicle privacy. At the same time, these models cannot guarantee the participants' truthfulness. For example, the malicious vehicles may deliberately claim a higher cost to maximize their payoff. This is because malicious vehicles attempt to take actions solely to guarantee their own payoffs. In addition, diversified vehicular resources make the incentive mechanism design more complicated. Most previous works consider the evaluation of the resources in an ambiguous way for simplicity [99], where they merely provide fixed monetary rewards for performing different kinds of tasks. This is not adequate to guarantee the fairness among vehicles. The utility brought by the sensing information is completely different with the storage or computing resources, and therefore we cannot measure them in the same way. Even within the same type of resource, the values can be different according to different characteristics. In addition, the security and privacy schemes of these works do not consider the privacy issues during announcement task.

Therefore, Yu *et al.* [94] proposed a reputation-aware task sub-delegation approach to identify reliable workers to delegate tasks in a crowdsourcing system. In addition, Boutsis and Kalogeraki [13] computed the reliability of workers and the probability that workers would execute tasks in time based on the characteristics of tasks and the profiles of workers. Therefore, this scheme can find a group of proper workers to perform tasks for customers.

An *et al.* [3] studied the credible crowdsourcing assignment model based on the social relationship cognition. They also proposed a service quality factor, link reliability factor, and region heat factor to evaluate the crowdsourcing preferences of workers for improving the accuracy of the task recommendations.

Xiao *et al.* [88] introduced an offline task assignment scheme and an online task recommendation algorithm following the mobility pattern of workers. Guo *et al.* [31] discussed the multi-task-oriented worker selection problem and proposed two task allocation frameworks to improve the efficiency of large-scale spatial crowdsourcing platforms. One is a worker selection framework based on workers' intentional movement for time-sensitive tasks, and the other is a task recommendation framework according to an unintentional movement for delay-tolerant tasks. Unfortunately, these schemes disclose the sensitive information to the cloud server to support the task recommendation.

Therefore, to resolve the privacy leakage, To *et al.* [81] introduced a framework to protect the locations of workers based on differential privacy and geocasting. This framework provides heuristics and optimizations to determine effective geocast regions for reaching a high task assignment ratio with a low overhead.

Shen *et al.* [73] proposed a secure task assignment protocol by utilizing the additive homomorphic encryption, which preserves worker's location privacy in a semi-honest adversary model. Consequently, Ni *et al.* [56] designed a privacy-preserving location matching scheme for spatial tasks in a mobile crowdsensing from matrix multiplication, in which the sensing area of the tasks and geographic location of workers are randomized by a random matrix to prevent the cloud server learned workers' locations. Besides, some privacy-preserving schemes [18] [19] have been designed from anonymity techniques to achieve the unlinkability between the identities of the workers and sensitive information disclosed during spatial crowdsourcing services.

Different from the above schemes, our scheme is able to select the competence of the vehicles without disclosing their private information, and it can ensure the confidentiality and integrity of the message simultaneously. In addition, the incentive mechanism is able to guarantee the fairness between vehicles in terms of payment. This is because the proposed incentive mechanism is more targeted that lets the participants to be more trustful. Thus, it can be resulted in a high welfare to both the cloud server and vehicles.

2.7.2 Signcryption Schemes

For achieving confidentiality, integrity, and authenticity simultaneously, signcryption scheme is used. The concept of the technique signcryption was first introduced by Zheng in [101]. The signcryption concept not only presents reduced computational costs but also has reduced communication overheads in comparison to the approach that requires signing and encrypting separately.

S.Moonseog *et al.* [71] proposed a domain-verifiable signcryption scheme, which is applied to the Electronic Funds Transfer (EFT) protocol. The scheme only predetermined n users within the domain that can decrypt their own part of a message and verify the whole transaction. After that, Malone-Lee [51] proposed the first identity-based signcryption scheme. Selvi *et al.* [67] developed an identity-based threshold signcryption scheme and formally proved its security in the existing security model.

Our privacy-preserving scheme mainly relies on the aggregation signcryption technique. The aggregation concept is a digital signature scheme, which was first proposed by Boneh and others [11]. The aggregate signature allows aggregation of different signatures by different users on different messages m_i. The primary objective of an aggregate signature scheme is to achieve both computation and communication efficiency. For example, when n users signed on n different messages, it is possible to aggregate all these signatures into a single signature.

Gentry *et al.* [28] developed an efficient identity-based aggregate signature scheme. This scheme can achieve full aggregation with a constant number of pairing operations during signature verification.

Selvi *et al.* [69] [70] analyzed the security in some aggregate signature schemes in [84] [85] and introduced two identity-based aggregate signature schemes. However, the authors did not present any proof for security. The scheme proposed in [69] cannot be considered an identity-based system because the public key of the user is not an identity-based public key.

Consequently, Selvi *et al.* [68] introduced the first aggregate signcryption scheme, where the researchers defined a comprehensive security model. The authors also, proposed some examples to prove how secure their method is by using random oracle models. Based on Selvi scheme, the author in [33] proposed an identity-based aggregate signcryption scheme as an appropriate secure model as has been proven in its use in the random oracle [8].

However, it seems that these schemes still need significant improvements over pairing maps used above. The Bilinear pairing operation is computationally intensive, leading these pairing-based schemes inefficient and impractical for VCC. Hence, in order to make the aggregate signcryption scheme more efficient compared to the existing schemes [33] [68], we introduce an efficient aggregate signcryption scheme, which is secure in the random oracle model [8].

2.7.3 Multiple Receiver Signcryption

In practice, broadcasting a message to multiple users in a secure and authenticated manner is an important facility for any manager who wants to communicate with a group of people working on the same project.

Thus, the first multiple receiver encryption concepts were introduced by Amos Fiat and Moni Naor [25] as a form of broadcast encryption. They identified and analyzed central message broadcasting problems to dynamically varying privileged user subsets in such a manner that non-privileged class is unable to learn about the message. Following this, various experts have proposed multiple broadcast encryption systems [32] [12].

Afterwards a number of papers also proposed multi-receiver signcryption system [71] [102], which is also now known as broadcast signcryption. The basic idea of these schemes is that the sender signcrypts n messages to n users. Each user can decrypt just his own message.

Li, Hu *et al.* [43] proposed a multi-receiver signcryption scheme based on bilinear pairing. However, these schemes are based on traditional public key cryptography.

Duan *et al.* [21] introduced the multi-receiver identity-based signcryption. However, Tan [79] showed that Duan *et al.*'s scheme is not secure against adaptively chosen ciphertext attacks under their defined security model.

Y.Yu *et al.* [97] proposed a new multi-receiver ID-based signcryption scheme. However, Selvi *et al.* [38] showed that Y.Yu *et al.*'s scheme does not satisfy the unforgeability and presented an improved scheme.

Accordingly, the multiple receiver identity-based signcryption scheme is emphasized in [83] [61] [98]. Thy are considered as an appropriate secure model and have been proven in its use in the random oracle model [8]. However, these schemes still suffer from increasing computational cost due to the increasing number of receivers. For example, consider that a sender wants to send a message to n receivers, which means he has to signcrypt the message n times for each receiver. Therefore, the increasing number of receivers leads to increasing computation cost.

2.7.4 Proxy Re-encryption

Proxy re-encryption is derived from the concept of decryption rights delegation, which was initially proposed by Mambo and Okamoto [52]. They gave some transformations that allow the original recipient to forward specific ciphertexts to another recipient.

After that, Blaze *et al.* [9] furthered the concept of decryption rights delegation through the idea of atomic proxy cryptography, in which a semi-trusted proxy computes a function that converts ciphertext for Alice into ciphertext for Bob without revealing the underlying plaintext. This scheme is only useful when the trust relationship between Alice and Bob is mutual.

S.Luo *et al.* [49], proposed two new unidirectional ID-based proxy re-encryption schemes, which are both proved secure in the standard model. The first scheme is a single-hop IB-PRE that allows the encryptor to decide whether the ciphertext can be re-encrypted. The second scheme is a multi-hop IB-PRE, which allows the ciphertext re-encrypted multiple times without increasing the size of ciphertext linearly.

Jun Shao [72] proposed the first anonymous ID-based proxy re-encryption (AIBPRE), which can be proven-secure in the random oracle model based on the decisional bilinear Diffie-Hellman assumption and modified decisional bilinear Diffie-Hellman assumption.

B.Libert *et al.* [45] present the first construction of unidirectional proxy re-encryption scheme with chosen ciphertext security in the standard model. The scheme construction is based on a reasonable complexity assumption in bilinear map groups.

In this thesis, we integrate the proxy re-encryption algorithm with the multiple receiver signcryption scheme in order to design a new and efficient multiple receiver proxy re-signcryption scheme. The scheme is able to eliminate the issue of increasing computational delay that results from increasing the number of receivers.

Chapter 3

A Privacy-preserving and Truthful Tendering Framework for Vehicle Cloud Computing

3.1 Introduction

Nowadays, vehicles are becoming more powerful and intelligent due to various powerful built-in sensors and on-board units [26]. Thus, S. Abdelhamid *et al.* [2] introduced a concept of *Vehicle as a Resource (VaaR)*, which focuses on making use of various vehicular resources such as *VaaR-Sensing* and *VaaR-Storage/Computing*. Inspired by $VaaS$, S. Olariu *et al.* [59] proposed *vehicle cloud computing* (VCC), which is an emerging vision of utilizing vehicular resources. The VCC system typically consists of a cloud platform and a number of vehicles with various capabilities. When there is a request for a task, a group of vehicles are recruited to accomplish it by bringing their resources together.

Nevertheless, adequate vehicle participation is critical to the success of VCC applications. A number of VCC applications have been proposed, which are based on the assumption that vehicles voluntarily contribute to the VCC. However, vehicles incur some cost when they provide their resources to the VCC. As a result, the vehicle owners may not be willing to participate unless they receive incentives such as compensation for their resources [4]. Thus, a well-designed incentive mechanism that stimulates vehicle participation is important. Some works use game theory such as *Stackelberg Game* to build incentive mechanisms [20] [91] [92] for vehicular resource procurement. However, these works provide a fixed monetary [20] reward which is not adequate to ensure vehicle participation. In addition, they assume the real cost of the vehicular resources is known to the VCC server, which is also impractical because the cost information is considered part of vehicle privacy. While that, the malicious vehicles may deliberately claim a higher cost to maximize their payoff because strategic vehicle owners would take actions solely to guarantee their own payoffs.

The fact that vehicles can provide diversified resources makes the incentive mechanism design more complicated. Most previous works that used game theory to stimulate vehicles owners valuate the vehicular resources in an ambiguous way for simplicity [99]. On the downside, the VCC may suffer with simplicity and ambiguity. For instance, the sensing information is totally different compared with the storage and computing resources, and hence we cannot measure them in the same way. Even within the same type of resource, the values can be different according to different characteristics. Obviously, we need an expressive way to clearly describe heterogeneous vehicular resources. We were inspired by a recent work [99], which creatively describes the resources in the traditional cloud with a heterogeneous language. We establish an expressive language that is capable of describing vehicular resources in the VCC system.

Motivated by several inherent advantages such as accurate pricing, many auction-based mechanisms have been proposed for cloud resource allocations. However, unlike these existing works, we propose a tendering-based incentive mechanism and adapt it to our vehicular resource procurement model. A tendering framework is a special type of auction in which the roles of buyer and seller are reversed, often referred to as a reverse auction. Most importantly, the tendering process is close to the way of how the VCC system works, where the cloud server prefers a lower cost for a task and participating vehicles seek to maximum rewards for their resources. In addition, the heterogeneous resources are described by our expressive language that is suitable for our tendering process. Nevertheless, to benefit from the tendering based heterogeneous resource procurement mechanism, we still need to overcome several challenges.

First, it is challenging to design a tendering framework that is compatible with heterogeneous vehicular resources, which is different from the traditional goods considered in a classic tendering process. Second, truthfulness is the major research effort for a tendering mechanism. It eliminates the overhead of gaming over each other and enables the VCC server to assign the tasks to the one with the highest value. A truthful mechanism helps us remove the burden of accurate pricing for vehicular resources and adapts the price to dynamic changing status. Third, truthfulness and privacy are somewhat contradictory objectives. We need to protect the privacy of truthful tenders during the process.

In this chapter, we aim at designing a truthful and privacy preserving tendering (TPPT) mechanism to solve the resource procurement problems in VCC. To the best of our knowledge, this is the first work that builds a secure incentive mechanism based on a tendering framework. The TPPT is resilient to strategic behaviors and preserves the tendering privacy at the same time. What is more, the assignment rule can select an optimal subset of heterogeneous vehicular resources with a minimum social cost. The main contributions are as follows:

- We design an illustrative language that is capable of describing heterogeneous vehicular resource types. Based on this, a tendering-based incentive framework is proposed to stimulate the participation of vehicles.
- We propose a *truthful privacy preserving tendering (TPPT) mechanism* that ensures truthful tenders and helps a VCC server selecting vehicles with optimal parameters for the task.
- We conduct a numerical analysis of the TPPT mechanism to validate the effectiveness. The results show that the proposed mechanism works effectively and guarantees the truthful tenders compared to the other schemes in [20] [91] [92].
- We design a signcryption technique with a homomorphic concept in order to preserve the truthful information reported by vehicles from being disclosed.
- We show the proposed privacy-preserving scheme is much more efficient in terms of computational costs and ciphertext size compared to the other signcryption schemes in [68] [33].

The remainder of the chapter is organized as follows. In Section 3.2, we present the system model and the problems for TPPT designing. Next, we solve the problems and build TPPT in Section 3.3. The security analysis of TPPT is presented in Section 3.4. Then, we give the results of simulation in Section 3.5. Finally, we draw our conclusion in Section 3.6.

3.2 System Model and Problem Formulation

In this section, we first present the general tendering model for vehicle recruiting. Then, we describe our language for heterogeneous vehicular resources. After that, we summarize the design problems for an efficient TPPT framework.

3.2.1 System Model of Resource Procurement

We consider that a general *Vehicle Cloud Computing* system consists of a VCC server, a roadside unit (RSU) and a number of vehicles denoted by $N = \{1, 2, ..., n\}$. The RSU acts as a gateway between a VCC server and vehicles. When the VCC server searches vehicles for resources, it sends a vehicle procurement message Φ to its connected RSU. The message includes the details of the task requirements, and may differ according to different resource types. Then, the RSU broadcasts this recruitment message to the vehicles under its range. The vehicles that are interested in participating in the campaign will respond to the recruitment message. The trusted authority (TA) is integrated into our system model, which is responsible for registering the vehicles and creating accounts for each of the registered vehicles to record their payments. The details of various tasks and required vehicular resources are described in *Section 3.2.2*. Next, we explain some key components in our resource procurement model:

Task — To finish a task, the VCC server needs to search vehicles to jointly fulfill the task with their vehicular resources. Φ specifies the resource requirements of the task.

Resource — Vehicular resources may differ between vehicles because of their different capabilities.

Cost — Vehicles incur extra operational costs for the resources. Let c_i denote the total cost of vehicle i for a given resource. Every vehicle expects a payoff larger than c_i. We should notice that c_i is private information for each vehicle i, and the owner does not want to reveal this value to others.

Tender — The vehicle that is participating in the procurement will submit a tender τ_i to the VCC server. It includes the claimed cost of the resource c_i' and the details of the resource it provides. We consider c_i' as the least payment that vehicle i claims to obtain by contributing its resource. Any strategic participant tends to reply that a c_i' is different from his true cost to maximize his payoff. We use $\Gamma = \{\tau_1, \tau_2, ..., \tau_n\}$ to describe the tender vector of all the participants.

Assignment Profile — After receiving the tender vector Γ, the VCC server needs to decide the task assignment profile $A = \{a_1, a_2, ..., a_n\}$. For vehicle i, $a_i = 1$ means assigned and $a_i = 0$ means not assigned. The VCC server chooses the vehicle based on tenders and the requirements of the task.

Payment profile — When distributing the tasks, the VCC server should also decide the payment for the vehicular resource. We have the payment profile $P = \{p_1, p_2, ..., p_n\}$ for all vehicles.

Utility — The utility $u_i(a_i)$ refers to the "net profit" tender i receives by finishing an assignment a_i. We can know that $u_i(a_i) = p_i - c_i$. As all vehicles are assumed to be rational, they will try to maximize their utility during the tendering process.

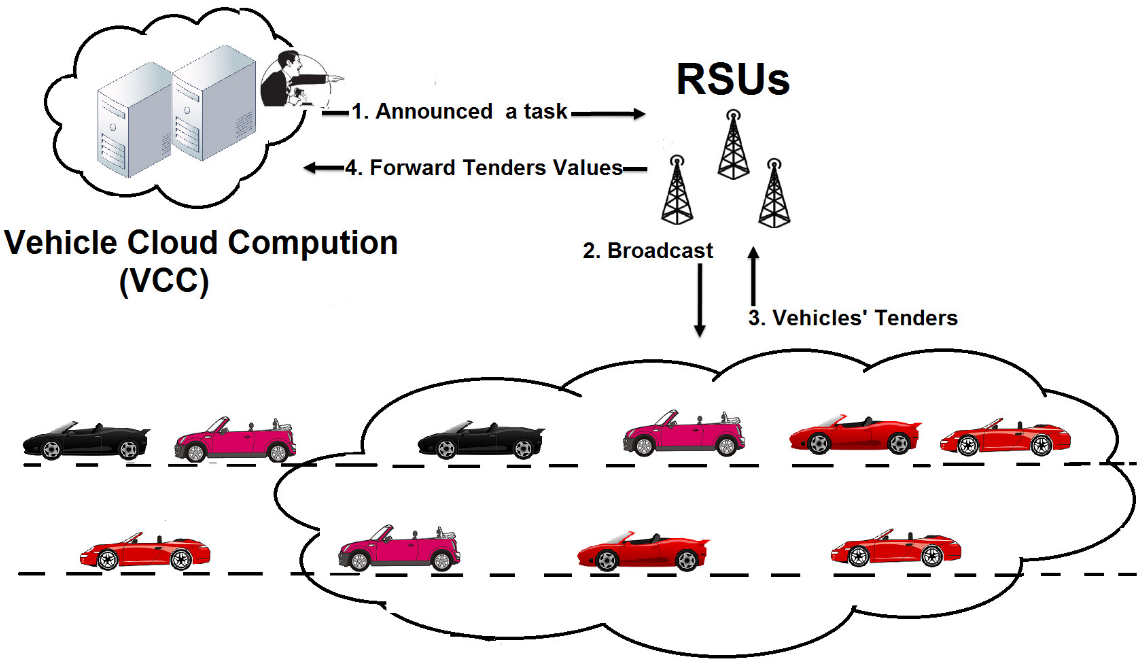

Figure 3.1: System Model.

As it illustrated in Fig. 3.1, we use a *tendering framework* to model the interactive process between the VCC server and vehicles by considering the VCC server as a tenderee and vehicles as tenderers. The interactions between the VCC server and vehicles are described as follows:

1. The VCC server advertises a task Φ to one of its connected RSU in the VCC system.
2. The RSU broadcasts the resource procurement message Φ to all vehicles under its range.
3. The vehicles that are interested in participating will reply with their tenders Γ.

4. Based on Γ, the VCC server jointly determine winning vehicles and their payments.

5. Wining vehicles perform the tasks and provide the corresponding resources to the VCC server.

6. Each vehicle i is paid an amount of money p_i for its wining tender τ_i.

The goal of tenderers is to maximize their utilities and tenderee aims to guarantee truthfulness and maximize task assignment efficiency subject to the complicated resource forms.

3.2.2 Description of Heterogeneous Resources

The vehicular resources are with different characteristics because of uneven vehicular capabilities. To make our system more practical, we categorize vehicular resources into two typical types (*VaaS-Sensing and Vaas-computing and storage*) and map them into a concise and unified form with an expressive language.

TYPE I: Sensing resource. Having a wide variety of sensors along with communication capabilities shapes the concept of *Vehicle Cloud Sensing*. This kind of application is very common and generates our first vehicular resource type, which is the sensing information from vehicle sensor devices [24] [86]. For a sensing task, the VCC server may need some information with regard to a location and a specific time period. For instance, a weather forecasting task needs various weather information such as temperature, wind and humidity for an appointed area and time.

TYPE II: Storage/computing resource. With powerful advanced in-vehicle computing power, it is foreseen that the VCC server will offload some computing tasks to vehicles [2]. In VCC, vehicle-generated data or data obtained from neighboring vehicles can be stored until the vehicle reaches a dedicated data collector or kept in the vehicle until retrieved as a reply to queries sent by data-seeking vehicles. This is different from traditional mobile crowdsensing, where each participating mobile device has limited computing power and more importantly is battery powered. For this kind of task, vehicles are chosen to provide storage/computing resources in a specific time period. Such requirement is widely seen in cloud market settings. For simplicity, we assume the amount of resources offered by a vehicle can meet the required amount of the task during its promised time period.

Given the above two different kinds of resources, our target is to design an expressive language that describes them in an uniform way. Both TYPE I and TYPE II tasks need resources along with some time and location requirements. The task procurement message $\Phi = \{RSC, t_s, t_e, l\}$ specifies the time period $[t_s, t_e]$ and location $l = (x, y)$ requirements for the resources RSC. RSC includes at least one resource request (e.g., TYPE I or TYPE II) and might be diverse with different task requirements. The vehicle can submit its tender if it is capable of supplying any required resource in Φ. We use $\tau_i = \{rsc_i, t_i(s), t_i(e), l_i, c_i'\}$ to represent the tender submitted by vehicle i. rsc_i represents the resources that vehicle wants to provide. Different vehicles may submit different resources rsc_i according to their various capabilities. rsc_i should include at least one type of resource. $[t_i(s), t_i(e)] \in [t_s, t_e]$ and $l_i = (x_i, y_i)$ denotes the time period and location for the resources from vehicle i. c_i' represents the declared cost of the resources and vehicles may cheat on this information, which means they might refuse to report their true cost c_i. Each vehicle is aware of its own resources' time period and location, through *Global Positioning System (GPS)* or other localization systems [63]. A vehicle should not misreport the location and time of the information in its tender. Misreporting may be detected easily and result in a serious penalty. The location difference of each information can be calculated as $d_i(l) = |l_i - l|$.

The VCC server makes the decision of vehicle selection and payment determination based on the tenders received. Most resources are time and location sensitive (e.g., the value of a resource is influenced by its time and location). This is reasonable for both TYPE I and TYPE II resources. Before announcing a task, the VCC server divides the time period into m time slots $t^* = (t_1^*, ..., t_m^*)$ as shown in Fig. 3.2, and we have $\sum_{i=1}^{m} t_i^* = t_e - t_s$. Thus, the time slots included by vehicle i are start from $\lfloor \frac{t_i(s) - t_s}{(t_e - t_s)/m} \rfloor + 2$ to $\lfloor \frac{t_i(e) - t_s}{(t_e - t_s)/m} \rfloor$. Different vehicles might have their time slots overlapped.

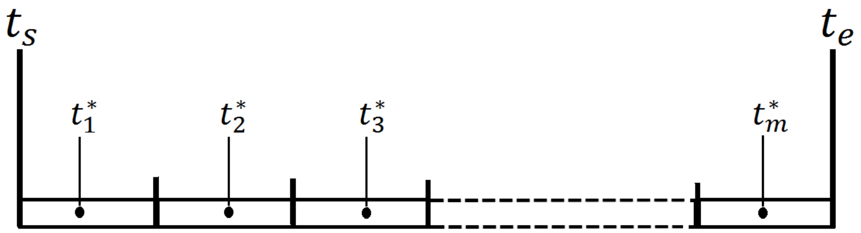

Figure 3.2: Dividing the time period into m time slots.

For each time slot, the VCC server targets to collect optimal resources from the closest location. *For different kind of resource, the VCC server only needs the optimal one for each time slot t_i^*, redundant resource will raise unnecessary costs. The VCC server hopes to choose a best resource combination for each time slot.* As illustrated in Fig. 3.3, the time interference and various vehicular resources makes the resource recruiting problem highly complicate.

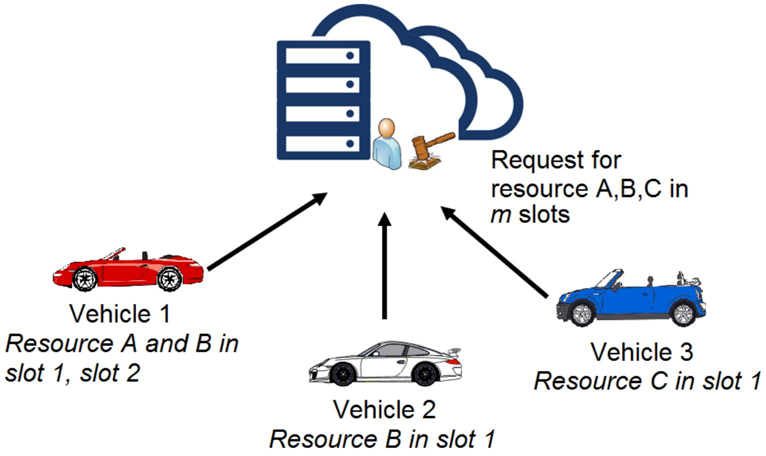

Figure 3.3: Illustration of conflict of all the available vehicular resources.

3.2.3 Problem Formulation

We first define some basic concepts for our tendering model. Then, we will discuss three challenges for TPPT design. Let s_i denote the tenderer i's preference strategy and s_{-i} be the strategy profile of all the players except for i. $u_i(s_i, s_{-i})$ is the utility of i when its strategy is s_i and the strategies of all other tenderers are s_{-i}. We have the following definitions.

Definition 1 *(Dominant Strategy). For any strategy $s_i' \neq s_i$, given other players' strategy profiles s_{-i}. We call s_i dominant strategy if the utility u_i of bidding s_i always satisfies the following condition:*

$$u_i(s_i, s_{-i}) \geq u_i(s_i', s_{-i}).$$

Definition 2 *(Incentive Compatible (also called Truthfulness)). A mechanism is* an incentive compatible *if reporting truth is the* dominate strategy *for all the tenderers.*

With *Incentive Compatible* guarantee, there is no incentive for any player to lie about his private information and no one can improve his utility by submitting a false tender. This guarantees player i's utility can be maximized by reporting its true cost, regardless of other players' strategy profiles s_{-i}.

Definition 3 *(Individual Rationality). A mechanism is individually rational if each player always gets a non-negative utility, which means that for any strategy s_i and any other players' strategy profiles s_{-i}, player i's utility is $u_i(s_i, s_{-i}) \geq 0$.*

The individual rational mechanism ensures that the cost of the vehicles can be covered. This serves as a basic condition for vehicle participation.

Definition 4 *(Monotonic Assignment). An assignment rule A is a monotone if the assignment $a_i(\tau_i, \tau_{-i})$ for vehicle i is monotonic decreasing with its claimed cost c_i'.*

Monotonicity in the tendering system means monotonic decreasing, which is the opposite way from the auction model. Monotonic assignment rule for tendering ensures that a vehicular resource with a lower cost can get more chances to be selected.

Definition 5 *(Welfare Maximization). In the reverse auction, welfare maximization means the assignment rule should minimize social cost $\sum_{i=1}^{n} c_i a_i$, where a_i is the amount of tasks assigned to the truthful tenderer i. This means the VCC server prefers to assign the task to the one who has a lower cost declaration.* [1]

Now, we propose the problems for the TPPT framework. For clarity, we assume there is a single resource request during each tendering process[2] in our discussion.

[1] In auction process, *Welfare Maximization* means auctioneer always allocates resources to the ones with higher bids [42].

[2] For multi-information request case, we can extend our assignment and charging algorithm to such scenario easily based on [104].

Problem 1. (*Winning Vehicles Determination Problem (WVDP)*). Given a pool of candidate vehicles N, the VCC server aims to gather the optimal vehicular resources that can cover as much time periods as possible with a minimum social cost,

$$A = argmin \sum_{i=1}^{n} a_i \cdot c'_i \; ; \; argmax \sum_{i=1}^{n} a_i \cdot (t_i(e) - t_i(s)).$$

The VCC server hopes to choose a best resource for each time slot. It prefers to the vehicular resources with a lower cost c_i and location difference $d_i(l)$. As discussed in *Section 3.2.2*, the optimal assignment rule design is complicated with heterogeneous vehicular resources. The fundamental reason is that the resources among vehicles are subjected to time interference constraints. Thus, we can easily deduce that these constraints make the problem NP-complete [104].

Theorem 1 *WVDP is NP-Complete.*

Proof: We start our proof by introducing an instance of the Minimum Set Cover (MSC) problem with an universe of k elements $U = \{\iota_1, ..., \iota_k\}$ and a set of n sets $H = \{h_1, ..., h_n\}$. The object of the MSC problem is to find the minimum-cardinality subset of H whose union contains all the elements in U. We construct k time slots $U' = \{t^*_1, ..., t^*_k\}$ based on U. Also, we construct h'_i from h_i, where h'_i is set of time slots belong to vehicle i. We aim to find the minimum-cardinality subset of $h'_i \in H'$ whose union covers all the required time period U'. Therefore, every instance of the NP-complete MSC problem is polynomial-time reducible to the modified WVDP problem.

Problem 2. *(Truthfulness Guarantee Problem (TGP)).* The tendering mechanism should ensure the incentive compatible and individual rationality. For each vehicle i, let τ'_i denote the untruthful tender. The utility for truthful and untruthful tenderers are $u_i(\tau_i, \tau_{-i})$ and $u_i(\tau'_i, \tau_{-i})$. The TGP is proposed to design a payment scheme that, for any vehicle i, we have:

$$u_i(\tau_i, \tau_{-i}) \geq u_i(\tau'_i, \tau_{-i})), \; and \; u_i \geq 0.$$

The vehicle's real cost c_i of performing the task is considered as a private information and should be unknown to others. Each vehicle owner is selfish and always wants to maximize his payoff. Thus, a vehicle i may manipulate c'_i for its own good. This kind of *strategic behavior* makes the VCC server difficult to decide the optimal vehicle set. Solving TGP can guarantee that vehicles declare their costs truthfully. This enables the tenderee to make decisions easily based on trustful tenders.

Problem 3. (*Privacy Preserving Problem* (PPP)). When vehicles report their true values, they do not want to share such sensitive information with the VCC server and other vehicles. Our system should protect the privacy of the truthful tender.

By solving this problem, we can make sure truthful tenders will not be revealed to the others. This will make our system trustful and give vehicles more confidence to act truthfully.

3.3 Design of TPPT

Aiming to design a privacy-preserving incentive scheme that solves the vehicular resource recruiting problem. TPPT consists of a computational efficient task assignment rule that can solve WVDP, a payment rule that helps to ensure truthfulness and a privacy-preserving scheme that can protect the true tenders of the vehicles. In this part, we will discuss them in details and present our TPPT.

3.3.1 Efficient Task Assignment Rule

We are trying to design a tendering mechanism with a two-step design paradigm. First of all, assume truthfulness without a justification, we strive to design a task assignment rule that enables a VCC server to select optimal parameters for a task. However, the NP-hardness of the problem prevents us from using the traditionally VCC mechanism, which requires that the optimal set of winners must be selected [24]. To achieve the desired property subject to computation efficiency, we describe interferences of vehicular resources as a conflict graph and then adopt a greedy algorithm to solve the problem.

If two resources overlap with more than one time slot, we consider them as conflict resources. We model the time conflicts of the tenderers as a conflict graph $\mathbb{G}(V, E)$, as shown in Fig. 3.4. The vertex represent the tenderers and two vertexes are connected if their time periods overlap. The VCC server only needs the optimal one from the conflict resources set for each time slot. The basic idea of greedy rule is to pick the next most cost-efficient tender that makes the ”greatest progress" towards finishing the task, and then deletes all its neighbors until no tenderers exist or the required time period is covered.

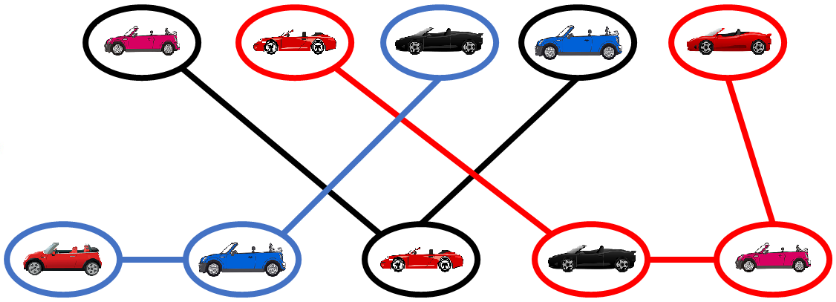

Figure 3.4: Modeling the time conflicts of the tenderers as a conflict graph $\mathbb{G}(V, E)$.

Suppose $c'_i = c_i$, the assignment rule A aims to choose a set S of winners with a maximum time coverage and a minimum social cost to finish the task. The process is as follows:

1. Sort the tenderers according to their cost values such that

$$c'_1 < c'_i < ... < c'_n.$$

The resource with a lower cost tends to be more valuable. It is worth knowing that the traditional mechanism only considers the resource cost when selecting winners. However, this step is not sufficient to select an optimal vehicle especially when some of the tenderers in the same group have the same social cost. For example,

$$(c'_1 = c'_2 = c'_i) < c'_{i+1} < ... < c'_n.$$

In this case, we perform step 2.

2. Sort the tenderers that have same cost in the same time slot such that

$$d_l(1)^\alpha \cdot c'_1 < d_l(2)^\alpha \cdot c'_2 < ... < d_l(i)^\alpha \cdot c'_i.$$

Then, select the resource with a lower location difference. α is the influence factor of the location difference. A small α makes the location difference more important.

3. Pick smallest in step one and/or two as winner and then delete all its neighbors in the sequence. Continue this step until $\sum_{i=1}^{n} a_i \cdot t_i^* \geq t_e - t_s$ or the tenderer sequence is empty.

Algorithm 1 describes our monotonic assignment procedure, where $\mathbb{A}$ denotes the tenders that are still available and $nbr(i)$ represents the neighbors of tenderer i.

Algorithm 1 Approximate Algorithm for TGP

```
Input: Task $\Phi$ and tender set $\Gamma = \{\tau_1, ..., \tau_n\}$.
Output: Assignment set $A = \{a_1, ..., a_n\}$.
$\mathbb{A} \leftarrow \Gamma$
for $i = 1 : n$ do
    $a_i = 0$;
end for
Sort tenders according to $c_i'$,
$c_1' < c_2' < ... < c_n'$,
if $c_1' = c_i'$ then
    Sort tenders sharing same cost according to their distance $d_l(i)^\alpha \cdot c_i'$,
    $d_l(1)^\alpha \cdot c_1' < d_l(i)^\alpha \cdot c_i' < ... < d_l(k)^\alpha \cdot c_k'$,
end if
while $\mathbb{A} \neq \emptyset$ do
    $i \leftarrow argmin(c_i')$
    $a_i = 1$
    $\mathbb{A} \leftarrow \mathbb{A} \backslash (nbr(i) \bigcup i)$
end while
return $A = \{a_1, a_2, ..., a_n\}$
```

Lemma 1 *Assuming truthfulness, the greedy assignment rule is a monotonic assignment.*

Proof: Suppose tender τ_i wins in the q-th iteration. In the previous iteration, a number of winning tenderers have been determined. We use a sorted list L storing these winning tenders in the order that they have been determined. Suppose τ_i is in the q-th place. Assume c_i replaced by $c_i' \leq c_i$, then tender τ_i' must have won in the q-th or an even earlier iteration. This proves the monotonicity of the assignment rule.

3.3.2 Computational Complexity

We now analyze the running time of our scheme for a given conflict graph $G = (V, E)$ with n tenderers and t^* time slots. First, the VCC server needs to examine all n tenderers to find the sets of k tenderers that share the same time slots. This process takes $k|E|$ time for n tenderers. The VCC server takes $O(k\ log\ k)$ time to sort the tenderers sharing same time slots. Second, the VCC server uses this sorted, and hence its complexity only comes from the process of finding vehicles with the lowest-cost in each $|E|$ for each time slot. Therefore, the overall complexity of the VCC server is $O(k|E|)$. Together, the overall complexity of the VCC server with strict requests is $O(k\ log\ k + |E|)$.

3.3.3 Critical Payment Scheme

Based on the greedy assignment rule, now we design a payment scheme to ensure truthfulness and individual rationality, such that each vehicle honestly reports its true cost in a tender.

Definition 6 *(Critical Neighbor [24] [42]). As shown in Fig. 3.5, for vehicle i, we call vehicle $i + 1$ the critical neighbor $nbr(i)^*$ of vehicle i if i's claimed cost is lower than $nbr(i)^*$, i will be assigned; else, it will be not assigned.*

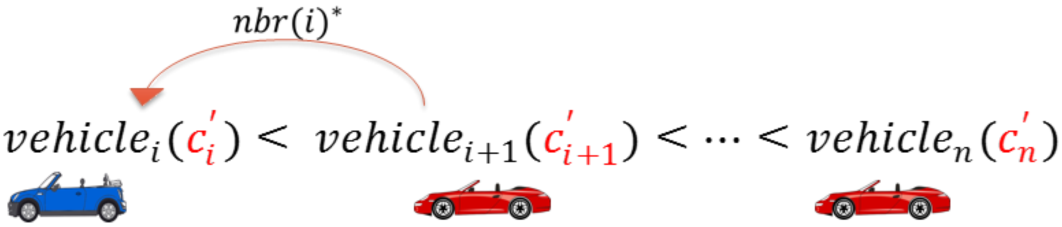
$nbr(i)^*$
$vehicle_i(c_i^{'}) < vehicle_{i+1}(c_{i+1}^{'}) < \cdots < vehicle_n(c_n^{'})$

Figure 3.5: Critical Neighbor

Definition 7 *(Critical Value [24] [42]). We call $c_{i+1}^{'}$ critical value c_i^* for vehicle i if i can only win by declaring a cost that is lower than c_i^*. In our Tendering model, it is represented by the claimed cost of i's critical neighbor.*

Lemma 2 *If the assignment rule satisfies monotonicity [42], then for each tenderer, there exists a critical value c_i^*. If $c_i > c_i^*$ it doesn't receive the task, else it does.*

Lemma 1 has shown the monotonicity of the assignment rule, we can know each tenderer i has a corresponding critical value according to *Lemma 2*, and hence we have $c_i^* > c_i$. The basic idea of finding critical tender is deleting τ_i and greedily selecting other tenders as shown in *Algorithm 1* until τ_i is useless. We use critical payment rule [24] [42] [57] for tendering to determine the payment for the winning vehicles. *Algorithm 2* describes our critical payment rule.

Definition 8 *(Critical payment rule). The critical value based payment scheme P can be defined as: $p_i = c_i^*$ if i wins and $p_i = c_i'$ otherwise.*

Lemma 3 *When the assignment rule satisfies monotonicity, the tendering mechanism is truthful if the VCC server pays the winning tenderers their critical values.*

Proof: When a mechanism has a monotone assignment rule accompanied with a critical payment rule, it is easy to demonstrate the truthfulness, according to [24] [42] [57].

Theorem 2 *TPPT satisfies truthfulness and individual rationality.*

Proof: The truthfulness can be deduced based on *Lemma 1-3*. According to the payment rule, the winning tenderer i is supposed to get paid with c_i^*, which is largest than its cost. The other tenderers who are not selected will get zero utility since they do not need to provide their resources. We can see all the tenderers will receive a non-negative utility by participating the tendering. Thus, the individual rationality can be proofed.

Algorithm 2 Critical Payment Determination Algorithm

Input: Assignment profile A tenderers N and conflict graph $\mathbb{G}$.

Output: Payment profile P

```
for $i = 1 : N$ do
    if $a_i = 0$ then
        $p_i = 0$
    else
        $\mathbb{A} \leftarrow N \setminus \{i\}$
        while $\mathbb{A} \neq \emptyset$ do
            $k \leftarrow argmin(c'_i)$
            if $k \in nbr(i)$ then
                $p_i = c'_k, nbr(i)^* = k$
            end if
            $\mathbb{A} \leftarrow \mathbb{A} \setminus (nbr(k)) \bigcup k)$
        end while
    end if
end for
return $P = \{p_1, p_2, ..., p_n\}$
```

3.3.4 Privacy-Preserving Scheme

In this work, we integrate the signcryption technique [101] with a homomorphic concept [27] in order to protect truthful tenders' information from being disclosed. Before introducing our cryptosystem scheme, we recall bilinear group, which is the bases of our privacy scheme.

Definition 9 *(Bilinear Group). Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic additive groups of the same prime order q. A mapping $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is called an admissible bilinear pairing if $(\hat{e})$ has the following properties:*

- *Bilinearity: For all $P, Q, V \in \mathbb{G}_1$ and $a, b \in Z_q^*$, we have*
    - $\hat{e}(P, Q + V) = \hat{e}(P, Q)\hat{e}(P, V)$.

  - $\hat{e}(P+Q, V) = \hat{e}(P, V)\hat{e}(Q, V)$.
  - $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab} = \hat{e}(bP, aQ)$.

- *Non-Degeneracy:* $P, Q \in \mathbb{G}_1$, *where*
  - $P \neq 0 \Rightarrow \hat{e}(P, Q) \in \mathbb{G}_2$.
  - $P \neq 0 \Rightarrow \hat{e}(P, Q) \neq 1$.

- *Computability:* $P, Q \in \mathbb{G}_1$, *there must exist an efficient polynomial time algorithm to compute* $\hat{e}(P, Q)$.

The admissible bilinear pairing $\hat{e}$ *can be implemented by either Weil/Tate pairings over elliptic curves [10].*

Complexity Assumptions

We assume the discrete logarithm problem related to our security proposal as follows.

Definition 10 *Computational Diffie-Hellman* (CDH) *Problem. Given* $P, aP, bP \in \mathbb{G}_1,\ \forall a, b \in Z_q^*$, *the* (CDH) *problem is to compute* $abP \in \mathbb{G}_1$ *probability within polynomial time.*

Definition 11 *Decisional Bilinear Diffie-Hellman* $(DBDH)$ *Problem. Given* $P, aP, bP, cP \in \mathbb{G}_1,\ \forall a, b, c \in Z_q^*$ *and* $f \in \mathbb{G}_2$, $DBDH$ *problem is to decide whether* $f = \hat{e}(P, P)^{abc}$.

3.3.5 Proposed TPPT Mechanism

In TPPT, tenderers submit their encrypted tenders to the connected RSU. Then, the RSU preprocesses them and sends the results to the VCC server (tenderee). The tenderee decrypts the processed ciphertexts and obtain only the necessary information to run the tendering process. The proposed scheme is based on a key-homomorphic concept and a signcryption technique. We present the design details of the TPPT as follows.

Phase 1: Initialization. The TA generates the bilinear parameters ($\mathbb{G}_1$, $\mathbb{G}_2$, P, $\hat{e}$, q) by given the security parameter κ. Then, it selects a large random prime number $s \in Z_q^*$ as a master private key and computes the corresponding public key P_{pub} = sP, where P is a generator of $\mathbb{G}_1$. Additionally, the TA determines three secure cryptographic hash functions: $H_1 : Z_q^* \to \{0,1\}^{256}$, $H_2 : \mathbb{G}_1 \to \{0,1\}^{256}$, $H_3 : \{0,1\}^{256} \to \mathbb{G}_1$. Therefore, the system public parameters published as $param = (\mathbb{G}_1, \mathbb{G}_2, q, P, \hat{e}, P_{pub}, H_1, H_2, H_3)$.

Phase 2: Key-Generation. Any vehicle i that wants to join the system, it should send its identity ID_i to the TA. In order to protect the vehicle's identity, the TA will generate a pseudo identity $Q_i = H_3(ID_i)$ for the vehicle i. Then, for each vehicle i, the TA selects a random number $x_i \to Z_q^*$ as vehicle i's private key and computes $pk_i = x_iP$ as vehicle i's public key. The public and private keys (pk_i, x_i) are sent to the vehicle i with its pseudo identity Q_i.

Phase 3: Tendering. Each vehicle i signcrypts its tender $\tau_i = \{rsc_i, t_i(s), t_i(e), l_i, c_i'\}$ values as the following. The vehicle i randomly selects $r_i \in Z_q^*$ and computes,

- $D_i = r_iP.$
- $C_i = r_ic_i'(pk_{vc} + P_{pub}).$
- $c_i'' = C_i/D_i.$
- $L_i = r_il_i(pk_{vc} + P_{pub}).$
- $l_i' = L_i/D_i.$
- $T_i = t_i^*P, where\ t_i^* = t_i(s), t_i(e).$
- $F_i = r_ipk_{vc}.$
- $U_i = (P_{pub} + T_i).$
- $Z_i = \dfrac{1}{r_i}U_i.$
- $S_i = r_i(pk_{rsu} + Z_i).$
- $R_i = H_1(c_i'', l_i', rsc_i).$
- $K_i = R_i \oplus H_2(F_i).$

- $h_i = H_3(K_i)$.
- $\sigma_i = (x_i + r_i)h_i$.
- $\alpha_i = (K_i, \sigma_i, D_i, S_i)$.

Thus, the vehicle i's cipheretext is α_i that will be sent to the RSU.

Phase 4: Aggregate-Verification. We adopt the aggregation technique in our proposed scheme to enable the RSU to aggregate all ciphertexts $(\alpha_i)_{i=1}^{n}$ into one ciphertext (α_{agg}) and verify them simultaneously. Whenever receiving $(\alpha_i)_{i=1}^{n}$, the RSU computes the following.

1. **Aggregation**. The RSU aggregates multiple of $(\alpha_i)_{i=1}^{n}$ into a single (α_{agg}) by performing the following steps.
   - Takes a collection of individual ciphertexts $\alpha_i = (K_i, \sigma_i, D_i, S_i)_{i=1}^{n}$, which are generated by vehicles with their pseudo identities $(Q_i)_{i=1}^{n}$ and corresponding public keys $(pk_i)_{i=1}^{n}$.
   - Computes the signature aggregation σ_{agg} = $\sum_{i=1}^{n} \sigma_i$.
   - Outputs the aggregate ciphertexts α_{agg} = $(K_1 ... K_n, D_1 ... D_n, S_1 ... S_n, \sigma_{agg})$.
2. **Batch Verification**. By given (σ_{agg}), pseudo identities $(Q_i)_{i=1}^{n}$ and corresponding public keys $(pk_i)_{i=1}^{n}$, the RSU computes $h_i = (H_3(K_i))_{i=1}^{n}$ and accepts the aggregation signature (σ_{agg}) if the following equation is valid.

   $$\hat{e}(P, \sigma_{agg}) \overset{?}{=} \hat{e}(\sum_{i=1}^{n}(pk_i + D_i), h_i).$$

   If the batch verification holds, the RSU will accept α_{agg} as a valid ciphertexts $\alpha_i = (K_i, \sigma_i, D_i, S_i)_{i=1}^{n}$. Then, the RSU will continue to complete the Phase 5.

- The correctness of our signature scheme is as follows.

$$\begin{aligned}\hat{e}(P, \sigma_{agg}) &= \hat{e}(\sum_{i=1}^{n} P, (x_i + r_i)h_i) \\ &= \hat{e}(\sum_{i=1}^{n}(x_i + r_i)P, h_i) \\ &= \hat{e}(\sum_{i=1}^{n}(x_iP + r_iP), h_i) \\ &= \hat{e}(\sum_{i=1}^{n}(pk_i + D_i), h_i)\end{aligned}$$

Phase 5: Preprocessing. It is worth to point out that the ciphertext helps to detect the vehicles that share the same time slot. In this step, the RSU objects to sort the vehicles that share the same time slot as follows.

- For each vehicle i, the RSU computes,

$$\begin{aligned}W_i &= \hat{e}(P_{pub}, S_i)\hat{e}(P_{pub}, x_{rsu}D_i)^{-1} \\ &= \hat{e}(P_{pub}, U_i)\end{aligned}$$

  Note that, the tenders that have same W values are share same time slot.

- Sorts the vehicles that share the same time slot as,

$$e_i = \{W_1, ..., W_m\}$$

Although these steps run by the RSU, the RSU knows nothing about the tenders' values because all the processes are running on the ciphertexts. The data collection and pre-processes are shown in Fig. 3.6. Where $E = \{e_1, ..., e_n\}$ denotes the collection of edges. The RSU then sends each e_i with their corresponding $(\widehat{\alpha_i})_{i=1}^{m}$ information to the VCC server. Where $\widehat{\alpha_i} = (R_i, \sigma_i, D_i)$.

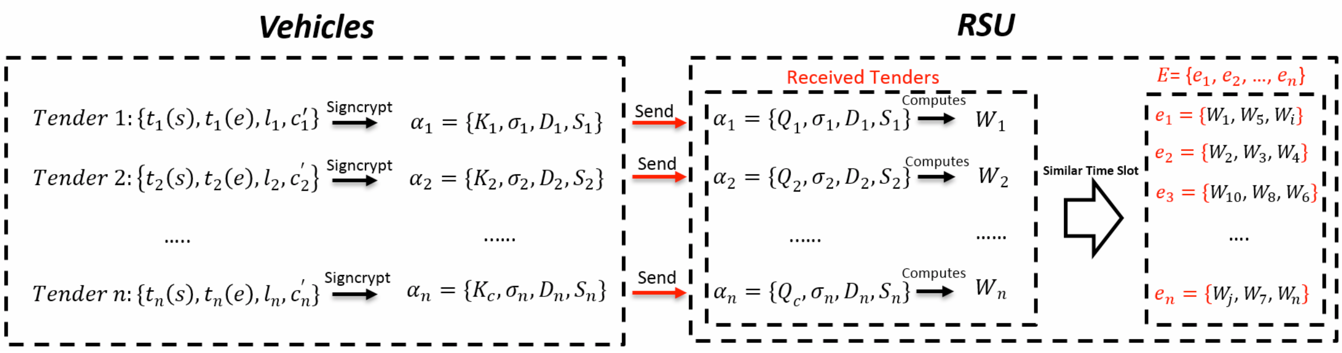
Vehicles
RSU
$Tender\ 1\colon \{t_1(s), t_1(e), l_1, c_1'\}$
Signcrypt
$\alpha_1 = \{K_1, \sigma_1, D_1, S_1\}$
$Tender\ 2\colon \{t_2(s), t_2(e), l_2, c_2'\}$
Signcrypt
$\alpha_2 = \{K_2, \sigma_2, D_2, S_2\}$
.....
......
$Tender\ n\colon \{t_n(s), t_n(e), l_n, c_n'\}$
Signcrypt
$\alpha_n = \{K_c, \sigma_n, D_n, S_n\}$
Send
Send
Send
Received Tenders
$\alpha_1 = \{Q_1, \sigma_1, D_1, S_1\}$
Computes
W_1
$\alpha_2 = \{Q_2, \sigma_2, D_2, S_2\}$
Computes
W_2
......
......
$\alpha_n = \{Q_c, \sigma_n, D_n, S_n\}$
Computes
W_n
Similar Time Slot
$E = \{e_1, e_2, ..., e_n\}$
$e_1 = \{W_1, W_5, W_i\}$
$e_2 = \{W_2, W_3, W_4\}$
$e_3 = \{W_{10}, W_8, W_6\}$
....
$e_n = \{W_j, W_7, W_n\}$

Figure 3.6: Homomorphic Preprocessing

- The correctness of W value is illustrated as follows.

$$\begin{aligned}
W_i &= \hat{e}(P_{pub}, S_i)\hat{e}(P_{pub}, x_{rsu}D_i)^{-1} \\
&= \hat{e}(P_{pub}, r_i(pk_{rsu} + Z_i))\hat{e}(P_{pub}, x_{rsu}r_iP)^{-1} \\
&= \hat{e}(P_{pub}, r_ipk_{rsu})\hat{e}(P_{pub}, r_iZ_i)\hat{e}(P_{pub}, x_{rsu}r_iP)^{-1} \\
&= \hat{e}(P_{pub}, r_ipk_{rsu})\hat{e}(P_{pub}, r_i\frac{1}{r_i}U_i)\hat{e}(P_{pub}, r_ipk_{rsu})^{-1} \\
&= \hat{e}(P_{pub}, U_i)
\end{aligned}$$

Phase 6: Tendering processing by a VCC server. After receiving the processed data $E = \{e_1, ..., e_n\}$ from the RSU, the VCC server determines the winners and their payments as the following steps:

- Conflict graph construction: After receiving E with their corresponding $(\widehat{\alpha}_i)_{i=1}^n$ information, the VCC server builds the conflict graph based on each vehicular resource's time period information as shown in Fig. 3.7.

- Monotonic task assignment: The VCC server uses his private key (x_{vc}) to start decrypt the ciphertexts $(\widehat{\alpha}_i)_{i=1}^n$ as follows.

  - $F_i' = x_{vc}D_i$.
  - $R_i' = K_i \oplus H_2(F_i')$.

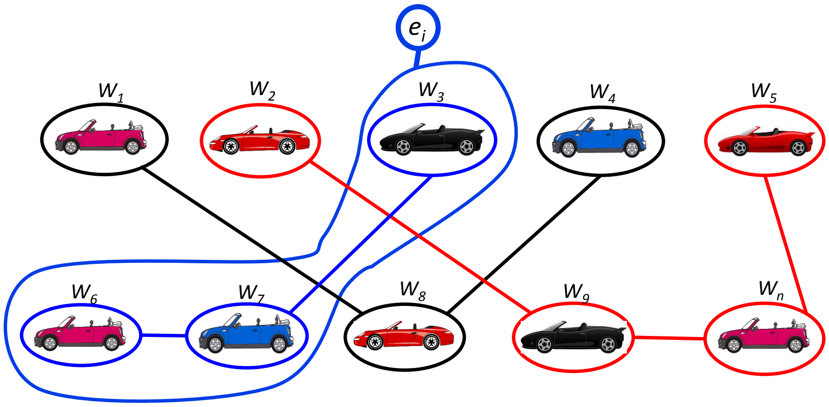

Figure 3.7: Sorting the tenderers that share the same time slot.

Then, it sorts them an ascending order according to their cost value c_i''. Where c_i'' is the encrypted value for c_i'. Thus, the VCC server will know nothing about the vehicle i's real cost c_i' value, even that after decrypting the ciphertext $\widehat{\alpha}_i$, and hence the vehicle i's privacy still in secure. If some vehicles in the same group e_i have the same cost c_i'' value, the VCC server will compute,

$$E(\tau_i) = c_i'' \cdot |(l_i') - (l)|^{\alpha}.$$

After that, the VCC server manipulates Algorithm 1 to determine the assignment vector A.

- Critical charging: The VCC server determines the critical neighbor $nbr(i)^*$ of the winner by running *Algorithm 2*. Then, the VCC server requests for the critical value from the RSU. The RSU replies with an encrypted message of the winner Q_i's critical value, $E(c_{nbr(i)^*})$. Finally, the VCC server decrypts the encrypted critical value for each winner and announces the assignment vector along with their payments.

- The correctness of our unsigncryption scheme is as follows.

$$\begin{aligned}
R_i' &= K_i \oplus H_2(F_i') \\
&= R_i \oplus H_2(F_i) \oplus H_2(F_i') \\
&= R_i \oplus H_2(r_i pk_{vc}) \oplus H_2(x_{vc} D_i) \\
&= R_i \oplus H_2(r_i pk_{vc}) \oplus H_2(x_{vc} r_i P) \\
&= R_i \oplus H_2(r_i pk_{vc}) \oplus H_2(r_i pk_{vc}) \\
&= R_i
\end{aligned}$$

- Then, the VCC server extracts (c_i'', l_i', rsc_i) values from R_i. Where c_i'' and $l_i' \rightarrow Z_q^*$, which are computed as follows.

$$\begin{aligned}
c_i'' &= \frac{C_i}{D_i} \\
&= \frac{r_i c_i'(pk_{vc} + P_{pub})}{D_i} \\
&= \frac{r_i c_i'(x_{vc} P + sP)}{D_i} \\
&= \frac{(r_i c_i' x_{vc} P + r_i c_i' sP)}{D_i} \\
&= \frac{(c_i' x_{vc} + c_i' s) r_i P}{D_i} \\
&= \frac{(c_i' x_{vc} + c_i' s) D_i}{D_i} \\
&= (c_i' x_{vc} + c_i' s)
\end{aligned}$$

3.4 Security Analysis

In this section, we briefly summarize the security properties of TPPT.

- *Security and Privacy Preservation.* In TPPT, we integrate a signcryption technique with a homomorphic concept to protect tenderers' privacy from being disclosed. Before submitting the tenders, the tenderer i signcrypts its tender value and sends it as a ciphertext (α_i) to the RSU. The RSU acts as a trustful intermediary agent. It pre-processes the encrypted tenders, and then sends the processed results $E_i = \{e_1, ..., e_i\}$ to the VCC server. The VCC server decrypts the ciphertexts and then starts running the tendering system by performing Algorithm 1 without knowing the cost c'_i during the tendering process. This is because the privacy of the vehicle's tender cost c'_i and location l_i are preserved under c''_i and l'_i.

- *Confidentiality and Integrity.* The proposed scheme guarantees the confidentiality and integrity of the message source. In line with Definition 1, the message is signed and encrypted under the CDH problem in order to achieve the confidentiality and integrity of the message. Thus, the adversary cannot decrypt any message without knowing the receiver's private key and r_i, which is randomly chosen from the sender and used to calculate $D_i = r_i P$ and $F_i = r_i(pk_{vc})$. In addition, the adversary cannot sign any message without having the sender's private key that is used to calculate $\sigma_i = (x_i + r_i)h_i$. As a result, only the receiver can decrypt the ciphertext by computing $F'_i = x_{vc} D_i$, where F'_i contains the receiver's private key. Therefore, according to Definition 1, the proposed scheme achieves confidentiality and integrity under the CDH problem.

- *Mutual Authentication.* The authentication phase is achieved by our proposed scheme, thanks to the signcryption technique. Under the scheme, the VCC server is authenticated by the signature on the message that is generated by the vehicle. In order to establish the mutual authentication, the sender calculates D_i, $F_i = r_i pk_{vc}$ and $\sigma_i = (x_i + r_i)h_i$, through the signcryption algorithm in the process of signcrypting the message (i.e. m_i). The receiver (VCC server) computes F'_i in order to establish the mutual authentication and authenticates the source report message by verifying the signature σ_i on receiving the ciphertext. Thus, the adversary cannot forge the signature on the message without knowing the sender's private key under the $DBDH$ problem.

3.5 Performance Evaluation

3.5.1 Performance of Privacy-Preserving

In this section, we analyse the performance of the proposed privacy-preserving scheme and compare it with the existing schemes in [33] [68]. We evaluate our proposed scheme in terms of the computational cost and communication overhead.

1. Computational Cost. In this case, a comparison is made between the scheme's efficiency and that of the aggregated signcryption schemes present in [33] [68]. Similar to the operations multiplication of a scalar in $\mathbb{G}_1$, $\mathbb{G}_2$ exponentiation and computation cost pairing, which are considered as the most important computation operations in time consumption computation. The comparison of computational costs among the schemes is shown in table 3.1. Where T_{pair} denotes the time consumption of pairing, T_{pmul} denotes the time consumption of a scalar point multiplication in $\mathbb{G}_1$ and T_{exp} denotes the time consumption of an exponentiation in $\mathbb{G}_2$. The proposed scheme algorithm takes 8 multiplication operations in $\mathbb{G}_1$ in order to compute the signcryption phase. In contrast, the unsigncryption phase takes one multiplication operation in $\mathbb{G}_1$ and three pairing operations in $\mathbb{G}_2$. Therefore, as shown in table 3.1, the computation cost in the proposed scheme is more efficient than existing schemes.

Table 3.1: Computation cost and communication overhead analysis

Scheme	Computation Cost	Communication Overhead
Y.Han et.al	$5T_{pair} + 4T_{pmult}$	$2\|\mathbb{G}_1\| + n\|m\| + n\|ID\|$
(IBAS_1)	$5T_{pair} + 3T_{pmult}$	$(n+1)\|\mathbb{G}_1\| + n\|m\| + n\|ID\|$
(IBAS_3)	$5T_{pair} + 6T_{pmult}$	$(n+2)\|\mathbb{G}_1\| + n\|m\| + n\|ID\|$
Proposed	$3T_{pair} + 9T_{pmult}$	$n(\|m\| + 2\|\mathbb{G}_1\|)$

The proposed privacy-preserving scheme efficiency of computation is done by using an MNT curve with Tate pairing, that is, $\hat{e}$: $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. This is defined over the employed curve, where the curves embedment degree is 6 and q is given as 160 bits. Intel Pentium IV 3.0 GHZ machine is used in the execution of the procedure [66]. The running time is displayed in table 3.2.

Table 3.2: Cryptographic operation running time

	Descriptions	Execution Time
T_{pmul}	Multiplication in $\mathbb{G}_1$	0.6 ms
T_{pair}	Pairing operation	4.5 ms

Fig. 3.8 shows the comparison of the computational cost between the existing schemes and our proposed scheme. The running time is given as $18.9\ ms$. As a result, the proposed scheme shows high efficiency and justification in relation to time.

2. Communication Overhead. The communication overhead is determined by the size of the ciphertext length. Here, we analyse the communication overhead of TPPT in two aspects, vehicle-to-RSU communication and RSU-to-VCC server communication. We first consider the vehicle-to-RSU communication, when a vehicle sends its tender value, it needs to send the encrypted tender value α_i to the RSU, which is $(|m| + 3|\mathbb{G}_1|)$. If we assume the binary length for each multiplication of the scalar point in $\mathbb{G}_1$ is 160 bits, we have $256 + 480$ bits for each α_i. Then, we consider the RSU-to-VCC server communication. After receiving the tender values, the RSU needs to find the sharing time slot e_i and forwards the $(\widehat{\alpha}_i)_{i=1}^m$ to the VCC server, which is $n(|m| + 2|\mathbb{G}_1|)$. The binary length of the encrypted $(\widehat{\alpha}_i)_{i=1}^m$ is $m(256 + 320)$ bits that can be increased with the growth of m. Table 3.1 shows that the proposed scheme reduces the communication overhead. By summarizing the above evaluations, we have an efficient protocol that has a lower computation time than other schemes, with a lower communication cost. Thus, our scheme is suitable for narrow bandwidth and terminals with limited resources.

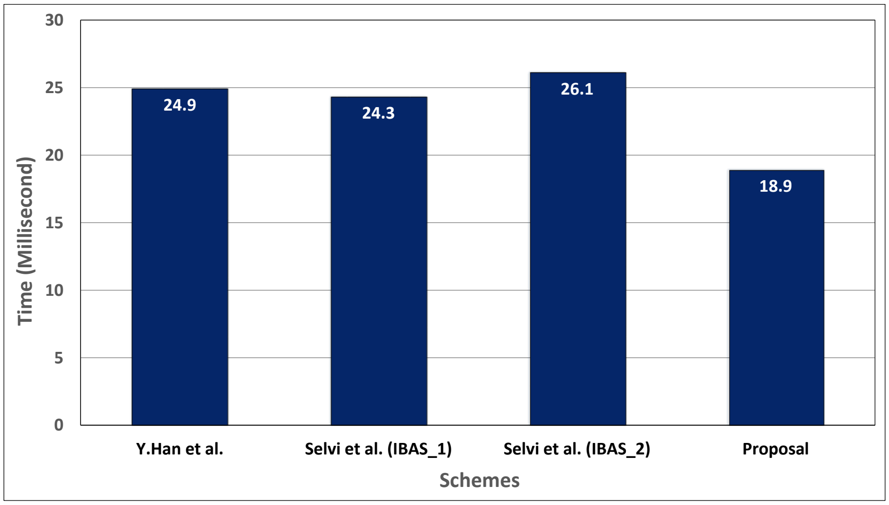

Figure 3.8: Efficiency comparison with other schemes.

3.5.2 Effectiveness Analysis of TPPT

In this section, we conduct extensive simulations to evaluate the performance of TPPT. We first demonstrate the truthfulness and individual rationality, and then we explore the property of TPPT in terms of social cost and satisfaction. As common practice, social cost is the total payments, and user satisfaction can be defined as the number of winning tenderers. While the VCC server satisfaction can be defined when the number of winning tenderers can cover all the required time periods. Thus, the users and VCC server satisfaction are considered as an important performance metric to measure the auction-based applications. We assume each tenderer's true cost is uniformly distributed over [5,15]. By default, the VCC server only has one kind of resource request for each task. We calculate the results average over 500 rounds.

In our simulation, we assume a single tenderee that handles tenderers in a geographic area. All tenderers are randomly deployed in a 50×50 square. Fig. 3.9 illustrates the utilities for each user under three different behaviors. In the experiment, we choose 100 vehicles, each of them holds vehicular resource with a random location and time slots. We set the time period requirement $[t_s, t_e]$ as 15 time slots. The untruthful claimed cost is measured by the ratio of the claimed cost to the true cost [86]. We can infer that vehicles always get more utilities from their truthful tenders. This guarantees that every rational tenderer will report their true value. It also shows that any vehicle will obtain nonnegative utility when submitting a true cost. Moreover, we can find that most untruthful higher tenderers get a zero utility. This is because most of them are excluded from the candidate's set with a high claim cost. Additionally, untruthful lower tenderers get a negative utility in some cases; this is because they win with a lower claimed cost but get a payment p_i that cannot be even balance off the cost of resource. By summarizing the above cases, the results show that our TPPT scheme works effectively and guarantees the truthfulness of users, compared to other game theory schemes such as Stackelberg in [20] [91] [92].

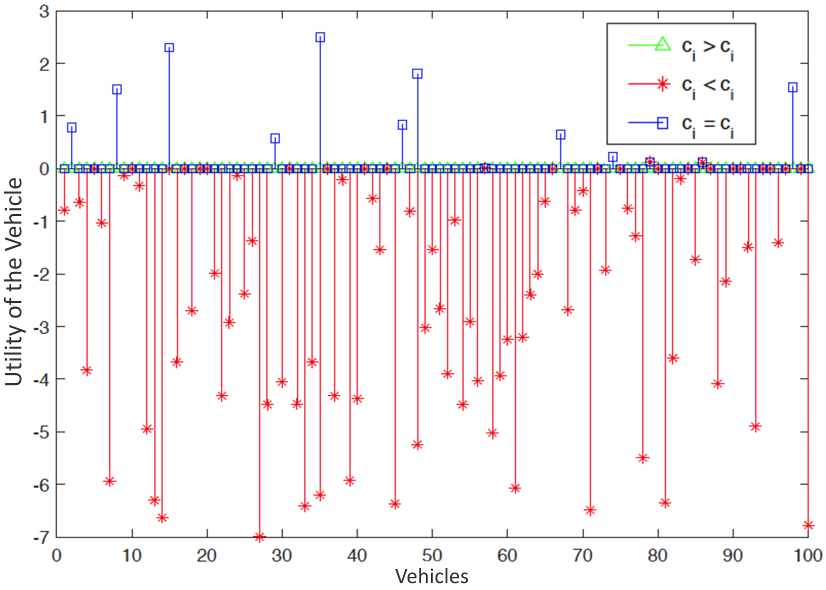

Figure 3.9: Verification of truthfulness and individual rationality

To explore the performance of our truthful incentive mechanism, we evaluate the user satisfaction and VCC server satisfaction of TPPT in Fig. 3.10 and Fig. 3.11 under three different time periods. We can infer that, the users and VCC server satisfaction are influenced by various number of the participating vehicles and time periods.

As shown in Fig. 3.10,the users satisfaction are influenced by various number of the time periods. We express the time period with different amount of time slots (i.e. 40,80,120). We can know that the number of winning vehicles is monotonic increasing with the change of participants and required time length. Thus, the user satisfactory increases when the required time period slots is increased. This is because the user has more chance to be selected as a winner. However, the difference is not obvious when the number of participants is small. This is because of a less diversity of vehicular resources caused by smaller participants and limited vehicular resource demands induced by a short time length.

In contrast, the VCC server becomes more satisfactory, as shown in Fig. 3.11, when the number of participants is large with small required time period. This is because the VCC server can find trustful users with a maximum time coverage and a minimum social cost to finish the task.

Fig. 3.12, depicts the performance of the social cost with a number of vehicles being varied from 10 to 200. At the beginning, the social cost increases because the number of recruited vehicles keep increasing. However, the social cost becomes steady or even shows a minor decline when the vehicles exceeds 120. This is because when there are more vehicles, the VCC server can find cheaper resources to perform the task. The general social cost increases with the time period. The difference is not obvious when the number of vehicles is less than 100. Because given the small quantity of participants, the time period of the vehicular resources are within a smaller range. Thus, the difference of winning vehicles is small.

Although the VCC server can find cheaper resources to perform the task when there are more vehicles, the issue is determined when some of the tenderers have the same social cost. Thus, we sort the tenderers that have the same cost according to their location distances such that $d_l(i-1)^\alpha \cdot c'_{i-1} < d_l(i)^\alpha \cdot c'_i < ... < d_l(k)^\alpha \cdot c'_k$. Fig. 3.13 shows the impact of α in vehicle's location. We set three fix values of α parameter to be (0.2, 0.5 and 0.9), and we fix the all vehicles' cost to be $\$10$. A vehicle with a near distance and a low cost tends to be more valuable. α is the impact factor of the location difference. The small α value makes the location more important.

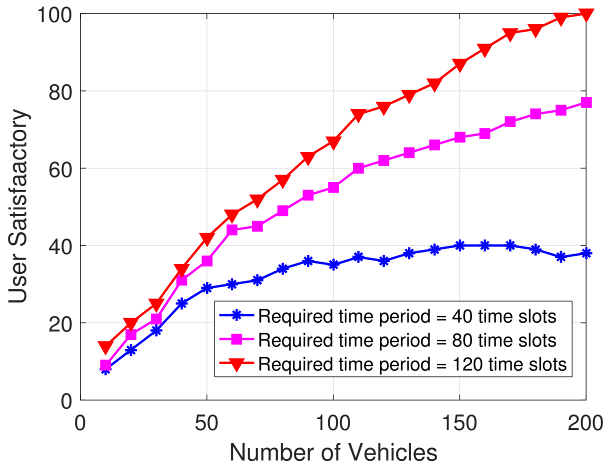

Figure 3.10: User Satisfaction

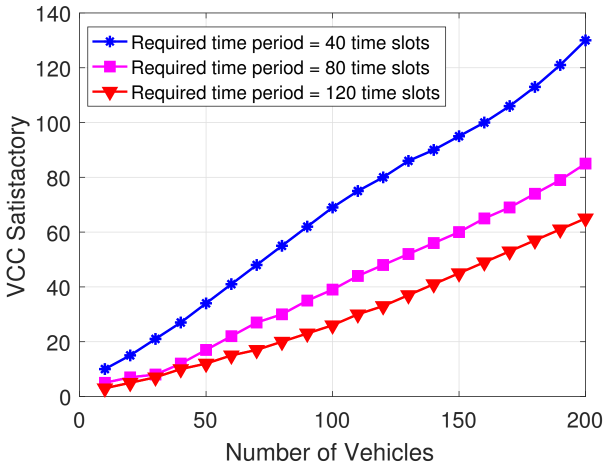

Figure 3.11: VCC Satisfaction

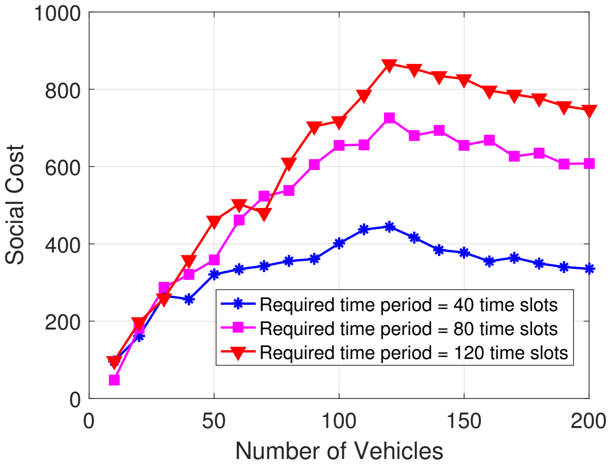

Figure 3.12: Social Cost

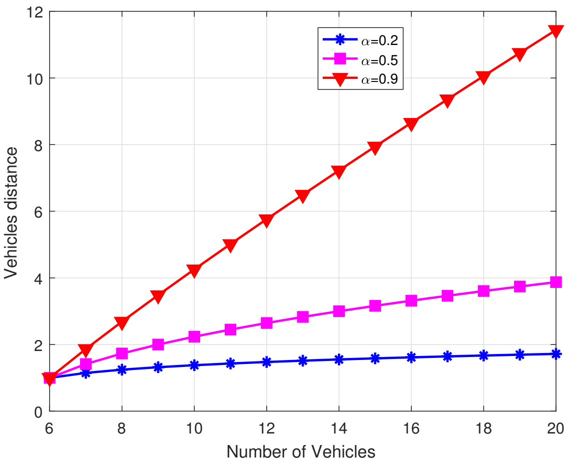

Figure 3.13: Distance

3.6 Conclusion

In this chapter, we solve the heterogeneous vehicular resource recruitments in the VCC system through the introduction of an innovative truthful tendering framework. It can minimize the social cost while satisfying a maximized time coverage. Unlike existing works, we describe various vehicular resources with our expressive language. Then, we present a greedy algorithm for heterogeneous vehicle selecting along with a payment rule that can ensure the truthfulness. At the same time we combine a homomorphic concept with a signcryption technique to protect vehicle's privacy. We confirm the truthfulness and evaluate the properties of the tendering mechanism with different simulations. In addition, we show the proposed privacy-preserving scheme is much more efficient in terms of computational costs and ciphertext size when compared to other signcryption schemes.

Chapter 4

Secure and Privacy-preserving Task Announcement In Vehicular Cloud

4.1 Introduction

Vehicular Cloud Computing (VCC) is a new paradigm that has a prominent impact on a traffic management and road safety [60]. In VCCs, a number of vehicles with abundant resources are viewed as service providers. These vehicles together can accomplish the tasks announcement by the VCC server. A typical VCC job processing procedure consists of a task announcement phase which is from the cloud server to the vehicles and a service providing phase when the vehicles send their sensing data to the cloud server. Accordingly, numerous VCC based applications have been proposed to make use of vehicles as resource providers in VCCs [60].

Although vehicles are considered as perfect candidates to provide various services, there still exist significant challenges in the real application of VCCs. The security issue is essential to the VCC system success. Specifically, the vehicles' privacy should be protected when they providing their services. Otherwise, it could be dangerous to vehicle owners. Consequently, the owners may choose to quit if they feel that their privacy cannot be guaranteed. Obviously, we need a well-designed privacy-preserving scheme to protect the vehicles' privacy in a VCC system. In light of this reality, some schemes have been proposed [47]. However, they only concentrate on privacy issues of the service providing phase by protecting the information from the vehicles to the VCC server. The task announcement phase seems to be neglected. Most existing frameworks assume the tasks can be simply sent out to the vehicle by the VCC server. Unfortunately, this may cause serious issues to the vehicles' privacy. As we know, a task issued by the VCC server often includes the details of what should be done by the vehicles. A vehicle that accepts the task has a high possibility to satisfy these requirements.

Without appropriate protection, these task requirements may also be manipulated by the adversary and cause privacy disclosure. Consider the following scenario, a cloud server hopes to broadcast several tasks with a specific location, time, etc. If all the tasks are sent without protection, any malicious individual can trace the tasks to a participating vehicle. Consequently, it can reveal the vehicle's trajectory by correlating multiple tasks accepted by the same vehicle. As a result, the vehicle's privacy could be compromised even though the vehicle is anonymous, for example, using pseudonym. This is because vehicle is driven by a person who usually has fixed daily routine. For example, going to work place at 9:00 am and coming back home at 6:00 pm. As illustrated in Fig. 4.1, the vehicle's daily routine is disclosed easily with the information of multiple tasks fulfilled by it. Obviously, the vehicle's privacy can be easily revealed knowing more tasks participated by it.

In order to fully protect the participants' privacy in VCC system, we need to ensure security and privacy of the information exchanged between the VCC server and vehicles at both task announcement phase and service providing phase. Unfortunately, little attention has been paid to privacy issues with task announcement in the VCC system. Nonetheless, for successful protection of announced task in VCC, we still need to overcome multiple challenges facing this emerging sector. Firstly, the challenge is not all about the authenticity of the source of an announced task but also extends to integrity as well as confidentiality of the announced task. Thus, it is important to design a security and privacy-preserving task announcement to guarantee that the announced task is not accessed or forged at the time of transmission by adversary. Secondly, such a system should allow for mutual authentication between the cloud server and vehicles. The system should be able to verify and decrypt the data simultaneously on low computational and communication costs. Finally, the system should be lightweight as a result of constraints in energy use and storage.

To successfully address the aforementioned issues, the multiple receiver signcryption technique [25] is used in pursuing the security objectives. This technique enables the broadcaster to sign and encrypt the message simultaneously for a specific number of receivers. It provides the most efficient solution to this dual problem of confidentiality, integrity and authentication. However, the multiple receiver signcryption technique is suffering from the issue of increasing the computational cost and time consumption that results from an increasing number of receivers. It is computationally intensive and leads to inefficient and impractical for VCC.

Motivated by the above mentioned issues, we aim to design an efficient privacy-preserving scheme for VCC based announced task management by integrating a multiple receiver signcryption technique with a proxy re-encryption technique. Our work is different from existing works [74] [62], as it provides vehicle's privacy, authenticity, confidentiality and integrity as well as data forward security for tasks announcement with saving computational cost and communication overhead. Concretely, vehicles and the VCC server communicate to each other via Roadside unit (RSU). With our proposed scheme, sensitive task messages can be securely and efficiently transmitted from the VCC server to vehicle(s). To be more specific, the main contributions of this scheme include:

- We first propose a new efficient multiple receiver proxy re-signcryption scheme (MRPRS) by combining signcryption and proxy re-encryption techniques. Our scheme eliminates the issue of increased computation delay that most multiple receiver signcryption schemes are suffering from, especially when the number of receivers become larger.
- Then, we use the proposed MRPRS as concealing technique to prevent the vehicles' privacy from being disclosed during the task announcement.
- The proposed scheme shows the efficiency in terms of computational costs and ciphertext size compared to existing multiple receiver signcryption schemes [83] [61] [98] and proxy re-encryption schemes in [49] [72] [45].

The rest of this chapter is organized as follows. In Section 4.2, we introduce the system model, security requirements, and design goals followed by its preliminaries in Section 4.3. In Section 4.4, the proposed MRPRS is presented in detail. In Section 4.5, we describe the secure and privacy-preserving task announcement in vehicular cloud. In Section 4.6, the security analysis is shown and performance evaluation is shown in Section 4.7, respectively. Finally, we draw our conclusion in Section 4.8.

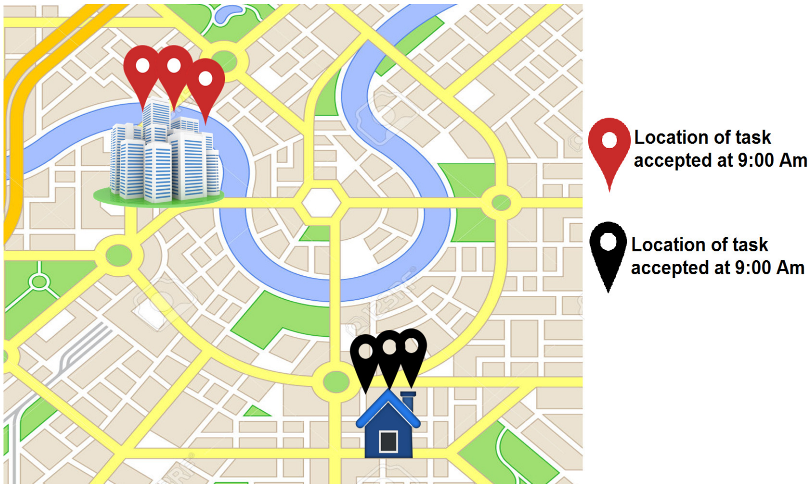
Location of task accepted at 9:00 Am
Location of task accepted at 9:00 Am

Figure 4.1: A simple trajectory and location-based inference attack on announced task in VCC.

4.2 System Model, Security Requirements and Design Goals

In this section, we introduce the system model, show the security requirements, and identify the design goals.

4.2.1 System Model

In our system model, we consider a general vehicular cloud service request framework. As shown in Fig. 4.2, the system consists of a VCC server, a roadside unit (RSU), a number of vehicles. When the VCC server needs to recruit vehicles for their resources, it will announce a task towards one of its connected RSUs. The task announcement always includes specific details of the task's requirements, and may differ according to different location and time. The RSU acts as a gateway between the VCC server and vehicles, it helps to direct the messages from the VCC server to vehicles and all messages from the vehicles to the VCC server. The vehicle that is interested in joining the announced task, it will respond with its parameter. The VCC server then chooses vehicles with optimal parameters to act as resource providers. A trusted authority (TA) is integrated into the VCC system, which is responsible for registration vehicles.

4.2.2 Security Requirements

In our security model, we focus our attention to the threat of the task announcement generated by the VCC server, which is then forwarded to the vehicles via RSU. Announced tasks devoid of content oriented privacy may result in disclosing the vehicle's privacy. For example, the adversaries or the malicious RSU can disclose the private information of the vehicles by eavesdropping on an announced task that includes specific requirements. Frequently accepting special tasks enable the adversary to trace vehicle and reveal its sensitive information such as location and lifestyle. Additionally, the malicious RSU can encroach on a vehicle's privacy by creating a fake task that includes specific requirements to disclose the privacy of any vehicle that responded on this forged task. Therefore, to prevent the adversary and malicious RSU from violating the vehicle's privacy during task announcement, the following security requirements should be satisfied.

- Data confidentiality should be provided. Ensuring that the announced task do not reveal sensitive information. Even if the adversary or RSU eavesdrops on the announced task, it cannot reveal the content of the message and cannot determine the message destination.
- Authentication and integrity should be provided. Data manipulation by unauthorized parties should be detected. Only the VCC server is in charge of issuing announced task messages to vehicles and only the authorized announced tasks from the VCC server can be accepted by vehicles.
- Vehicle's privacy should be protected. Protection of vehicle's identity and location is of a paramount importance in the VCC system.

4.2.3 Design Goals

Our design goal is to propose a lightweight privacy-preserving scheme for a task management system to achieve the above security requirements. Specifically, the goals that are to be achieved are as follows.

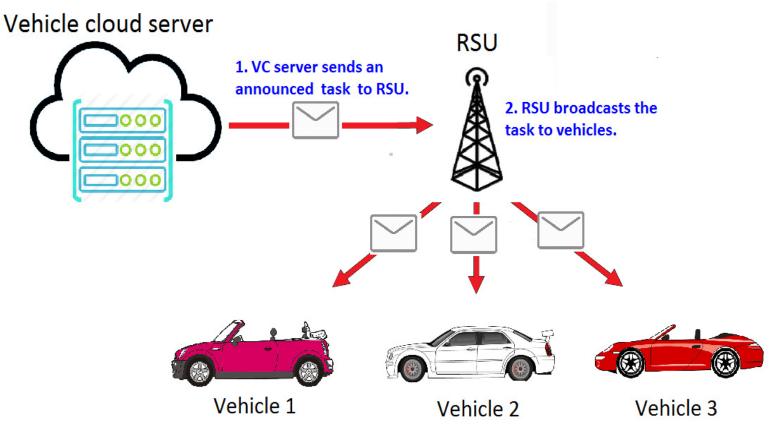
Vehicle cloud server
1. VC server sends an announced task to RSU.
RSU
2. RSU broadcasts the task to vehicles.
Vehicle 1
Vehicle 2
Vehicle 3

Figure 4.2: A Task Announcement Model in Vehicular Cloud.

- Privacy-preservation: The proposed scheme should provide data integrity and authentication as well as data confidentiality. This involves the ability to authenticate the source of the message and to ensure the integrity of the message with guarantee that the forwarded message does not reveal sensitive information of the message. In addition, the proposed scheme should protect the personal information of the participant during the authentication and forwarding process.
- Efficiency: The proposed scheme should also be efficient in terms of computation cost and the communication overhead compared to existing schemes.

4.3 Preliminaries

4.3.1 Bilinear Maps

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two multiplicative cyclic groups with same prime order q. A mapping $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is called an admissible bilinear pairing if $(\hat{e})$ has the following properties:

- Bilinearity: For all $Q, V \in \mathbb{G}_1$ and $a, b \in Z_q^*$, we have,
  $\hat{e}(V^a, Q^b) = \hat{e}(V, Q)^{ab} = \hat{e}(V^b, Q^a)$.

- Symmetric: $\hat{e}(V, Q) = \hat{e}(Q, V)$.
- Non-Degeneracy: $\hat{e}(V, Q) \neq 1_{\mathbb{G}_2}, where\ V, Q \neq 1_{\mathbb{G}_2}$.
- Computability: There is an efficient algorithm to compute $\hat{e}(V, Q)$.

The admissible bilinear pairing $\hat{e}$ can be implemented by either Weil/Tate pairings over elliptic curves [10].

4.3.2 Complexity Assumptions

We assume the discrete logarithm problem that related to our security proposal as follows.

- **Definition 1:** Computational Diffie-Hellman (CDH) Problem. Given $g, g^a, g^b \in \mathbb{G}_1,\ \forall a, b \in Z_q^*$, the CDH problem is to compute $g^{ab} \in \mathbb{G}_1$.
- **Definition 2:** Decisional Bilinear Diffie-Hellman (DBDH) Problem. Given $g, g^a, g^b, g^c \in \mathbb{G}_1,\ \forall a, b, c \in Z_q^*$, the DBDH problem is to decide whether $f = \hat{e}(g, g)^{abc}$, where $f \in \mathbb{G}_2$.

4.4 Proposed MRPRS Scheme

In this section, we propose an efficient MRPRS scheme, which serves as basis of our secure and privacy-preserving task announcement. The proposed scheme is based on multiple receiver signcryption schemes in [83] [61] [98]. However, their schemes are suffering from increased computational cost, as the number of receivers increase. We address this problem by integrating the proxy re-encryption with multiple receiver signcryption. Our scheme lets the sender to signcrypt the message just one time, which is signcrypting the message to himself and delegates number n of receivers to open it instead of signcrypting the message n time to n receivers. The proposed MRPRS scheme is composed by the following algorithms.

- *System setup(λ).* This algorithm runs by the TA. Given the security parameter λ, the TA chooses $\mathbb{G}_1$ and $\mathbb{G}_2$ as finite multiplicative cyclic groups with the same prime order q, g is a generator of $\mathbb{G}_1$, and a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. The TA determines three secure cryptographic hash functions: $H_1 : \mathbb{G}_1 \rightarrow Z_q^*$, $H_2 : \mathbb{G}_1 \rightarrow \{0, 1\}^*$ and $H_3 : \{0, 1\}^* \rightarrow \mathbb{G}_1$. The system public parameters published as $param$ = ($\mathbb{G}_1$, $\mathbb{G}_2$, q, g, $\hat{e}$, H_1, H_2, H_3).

- *Key-Generation($param, ID_i$).* This algorithm runs by the TA. For each user i, the TA selects a random number $x_i \in Z_q^*$ as user i's private key, and computes the corresponding public key X_i = g^{x_i}. Then, (X_i, x_i) will be sent to the user i in a secure manner.

- *Signcryption(X_s, x_s, m).* This algorithm runs by the sender ID_s to signcrypt the message $m_i \in M$. The sender ID_s randomly selects $r_i, v_i \in Z_q^*$ and computes,

  - $E_i = (X_s)^{r_i}$.
  - $V_i = g^{v_i r_i}$.
  - $F_i = H_2(V_i) \oplus m_i$.
  - $Z_i = H_3(F_i)$.
  - $\sigma_i = (Z_i \cdot E_i)^{x_s}$.

- *Re-key($x_s, (X_i)_{i=1}^n$).* This algorithm runs by the sender ID_s to compute the Re-key and delegates to a number of receivers as follows,

  - $T_i = g^{r_i}$.
  - $h_i = H_1(T_i)$.
  - $Rk_{s \to R} = \frac{h_i * v_i}{x_s}$.
  - $U_j = (X_j)^{r_i}$, for $(j = 1, ..., n)$.
  - Return the ciphertext $\alpha_i = (E_i, F_i, \sigma_i, U_1, ..., U_n)$, and Re-key ($Rk_{s \to R}$).

- *Re-signcryption(Rk, x_{px}, σ).* This algorithm runs by the proxy ID_{px} to re-signcrypt the message as follows.

  - $E_i' = (E_i)^{Rk_{s \to R}} = (X_s^{r_i})^{\frac{h_i v_i}{x_s}} = (g^{x_s r_i})^{\frac{h_i v_i}{x_s}} = g^{r_i h_i v_i}$.
  - $\sigma_i' = (E_i')^{x_{px}} \cdot \sigma_i$.
  - Return $\alpha_i' = (E_i', F_i, \sigma_i', U_1, ..., U_n)$.

- *Verification(σ_i').* This algorithm runs by the receive ID_i. The receiver ID_i verifies if the following equation holds outputs true otherwise false.

$$\hat{e}(g, \sigma_i') \stackrel{?}{=} \hat{e}(X_{px}, E_i')\hat{e}(X_s, (Z_i \cdot E_i)).$$

- *Unsigncryption(x_i, σ'_i).* This algorithm runs by the receive ID_i. If the output of the verification is true, the receiver ID_i will decrypt the message as follows,
  - $T'_i = U_i^{\frac{1}{x_i}}$.
  - $h'_i = H_1(T'_i)$.
  - $V'_i = (E'_i)^{\frac{1}{h'_i}}$.
  - $m' = F_i \oplus H_2(V'_i)$.
- The correctness of our signature scheme is as follows:

$$\begin{aligned}\hat{e}(g, \sigma'_i) &= \hat{e}(g, (E'_i)^{x_{px}} \cdot \sigma_i) \\ &= \hat{e}(g, (E'_i)^{x_{px}})\hat{e}(g, \sigma_i) \\ &= \hat{e}(g, (E'_i)^{x_{px}})\hat{e}(g, (Z_i \cdot E_i)^{x_s}) \\ &= \hat{e}(g^{x_{px}}, E'_i)\hat{e}(g^{x_s}, (Z_i \cdot E_i)) \\ &= \hat{e}(X_{px}, E'_i)\hat{e}(X_s, (Z_i \cdot E_i))\end{aligned}$$

- The correctness of $T'_i = T_i$ is as follows:

$$\begin{aligned}T'_i &= U_i^{\frac{1}{x_i}} \\ &= (X_i^{r_i})^{\frac{1}{x_i}} \\ &= (g^{x_i r_i})^{\frac{1}{x_i}} \\ &= (g^{r_i}) = T_i\end{aligned}$$

- The correctness of $V'_i = V_i$ is as follows:

$$\begin{aligned}V'_i &= (E'_i)^{\frac{1}{h'_i}} \\ &= (g_i^{r_i v_i h_i})^{\frac{1}{h'_i}} \\ &= (g_i^{r_i v_i H_1(T_i)})^{\frac{1}{H_1(T'_i)}} \\ &= (g_i^{r_i v_i}) = V_i\end{aligned}$$

- The correctness of unsigncryption is as follows:

$$\begin{aligned} m'_i &= F_i \oplus H_2(V'_i) \\ &= H_2(V_i) \oplus m_i \oplus H_2(V'_i) \\ &= m_i \end{aligned}$$

4.5 Secure and Privacy-preserving Task Announcement

In this section, we present the details of our secure and privacy-preserving task announcement. In VCC system, the VCC server sends a requirement task announcement to vehicles via RSU in order to recruit vehicles for their resources. These type of messages can be exploited by an adversary or even malicious RSU to disclose private data of the vehicles. Therefore, in order to protect the participants' privacy in VCC system during announced tasks, we designed a secure and privacy-preserving task announcement based on our proposed MRPRS scheme. In this application scenario, the VCC server signcrypts the message and delegates number of vehicles to decrypt it. The RSU is considered as a semi-proxy who is responsible to re-signcrypt the message and then forward it to the all vehicles under its communication range. The vehicles verify the signature on the receiving message and only the delegated vehicles are able to unsigncrypt the ciphertext. The proposed MRPRS scheme is introduced in the task announcement to fulfill the design objectives. The protocol consists as the following.

- **System Initialization**. Given the security parameter λ, the TA is responsible to publish $param$ = ($\mathbb{G}_1$, $\mathbb{G}_2$, q, g, $\hat{e}$, H_1, H_2, H_3) as we described in *System setup* in Section 4.4.
- **Registration and Key Generation**. For each vehicle i, the TA selects a random number $x_i \in Z_q^*$ and computes X_i = g^{x_i} as vehicle i's private/public keys. Then, the TA returns X_i and x_i to the vehicle i.

  Remark. In order to protect the vehicle i's identity privacy, the TA generates a pseudo identity $Q_i = H_3(ID_i)$ and publishes it with the vehicle i's public/private keys. Notably, as the VCC server and RSU are public institutions, it is not necessary to protect their identities privacy.

- **Data formulation and sending**. When the VCC server searches vehicles for collaboration, it will deliver the content of the announced task with its specifications towards the RSU. The VCC server authenticates itself to the vehicles and protects the content of the announced task from any malicious RSU or adversaries by signcrypting the task message m_i through performing the *Signcryption* phase in Section 4.4.

  $$Signcryption(X_s, x_s, m_i).$$

  Assume the VCC server has a complete knowledge about the vehicles within the coverage area in each RSU. Thus, the VCC server will generate a Re-key and delegates a number of registered vehicles to decrypt the ciphertext message as described in Section 4.4.

  $$Re - key(x_s, (X_i)_{i=1}^{n}).$$

  Then, the VCC server sends the ciphertext $\alpha_i = (E_i, F_i, \sigma_i, U_1, ..., U_n)$ with $Rk_{s \to v}$ to its connected RSU.

- **Data transmission**. After receiving the ciphertext α_i from the VCC server, the RSU will use its private key x_r with the re-encryption key $(Rk_{s \to v})$ to re-signcrypt the ciphertext α_i as follows.

  $$Re - signcryption(Rk_{s \to v}, x_r, \sigma).$$

  Then, the RSU broadcasts the $\alpha'_i = (E'_i, F_i, \sigma'_i, U_1, ..., U_n)$ to all vehicles within its communication range.

- **Verification**. Once the vehicles receive the α'_i, they will verify the σ'_i and accept α'_i if the following equation holds.

  $$\hat{e}(g, \sigma'_i) \overset{?}{=} \hat{e}(X_r, E'_i)\hat{e}(X_s, (Z_i \cdot E_i)).$$

- **Data receiving**. If the verification is valid; then, each vehicle i uses its private key x_i with its U_i value to continue the decryption α'_i as we described in 4.4 Section.

  $$Unsigncryption(x_i, \sigma'_i).$$

  Fig. 4.3, illustrates the secure and privacy-preserving task announcement in the VCC system.

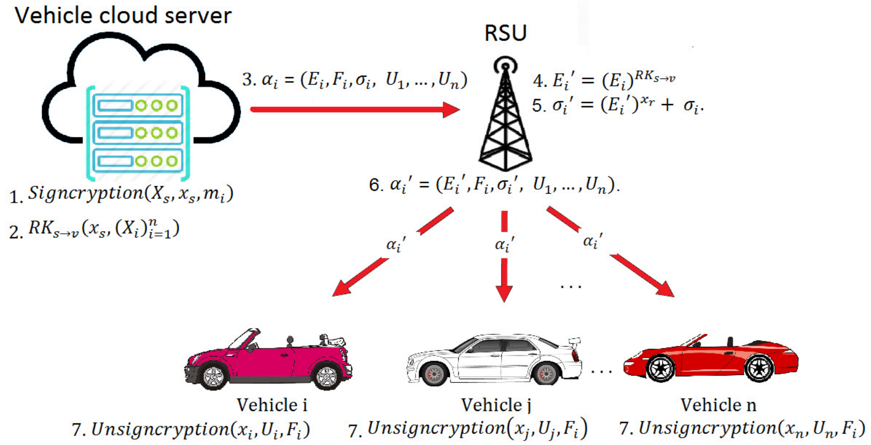
Vehicle cloud server
RSU
3. $\alpha_i = (E_i, F_i, \sigma_i, U_1, \ldots, U_n)$
4. $E_i{}' = (E_i)^{RK_{s\to v}}$
5. $\sigma_i{}' = (E_i{}')^{x_r} + \sigma_i$.
1. $Signcryption(X_s, x_s, m_i)$
2. $RK_{s\to v}(x_s, (X_i)_{i=1}^n)$
6. $\alpha_i{}' = (E_i{}', F_i, \sigma_i{}', U_1, \ldots, U_n)$.
$\alpha_i{}'$
$\alpha_i{}'$
$\alpha_i{}'$
. . .
Vehicle i
7. $Unsigncryption(x_i, U_i, F_i)$
Vehicle j
7. $Unsigncryption(x_j, U_j, F_i)$
Vehicle n
7. $Unsigncryption(x_n, U_n, F_i)$

Figure 4.3: Secure and Privacy-preserving Task Announcement.

4.6 Security Analysis

In this section, we analyze how the proposed MRPRS scheme achieves the design goals in Section 4.2.

- The proposed scheme can provide confidentiality and integrity for the task announcement in the VCC system. The message is signed and encrypted under definition 1 (CHD) problem, which is secure in the random oracle model [8]. Thus, the adversary cannot decrypt any message without knowing the receiver private key and r, v which are randomly chosen from the VCC server and used to compute $V = g^{rv}, T = g^r$. Also, the adversary cannot sign and re-sign any message without having the VCC server and RSU private keys. Since the proposed scheme employs a random integer in encryption and signature, it can resist the possible replay attack. Thus, using our proposed scheme we fulfills the goal of protecting task announcement against tracing and forgery attack.
- The proposed scheme can provide authentication. Under (DBDH) problem, the vehicle i authenticates the source of the task message by verifying the signature σ_i' on the receiving ciphertext.

- The proposed scheme can provide vehicle's data privacy preservation. The RSU and other participating vehicles know nothing about the content of the message and destination, which guarantees privacy preservation. Although the RSU re-signcrypts the task message, it is still unable to learn anything about the destination and contact of the message.

4.7 Performance Evaluation

In this section, we evaluate the performance of our proposed scheme in terms of the computational cost and communication overhead. As the operations of bilinear pairing and exponentiation in $\mathbb{G}_1$ and exponentiation in $\mathbb{G}_2$ dominate the computational overhead of the algorithms, we mainly consider the time consumption of these operations. Due to the fact that our proposed MR-PRS scheme combines the multiple receiver signcryption algorithm with proxy re-encryption, we compare it with the existing proxy re-encryption schemes in [49] [72] [45] and with other multiple receivers signcryption schemes in [83] [61] [98].

Table 4.1: Cryptographic operation comparison with other schemes.

Scheme	$Encrypt$	$RK-Gen$	$Re-Encrypt$	$Decrypt$
[45]	$3t_1+t_p+t_2$	t_1	$4t_1+2t_p$	t_p+t_2
[72]	$3t_1+t_p+t_2$	$2t_1+t_p+t_2$	$6t_p$	t_1+2t_p
[49]	$4t_1+t_p+t_2$	$3t_1$	$2t_p+t_2$	$2t_p$
Proposed	$3t_1$	$2t_1$	$2t_1$	$2t_1+3t_p$

1. Computational Cost.
   a) In this case, a comparison is made between our scheme and the other proxy re-encryption schemes present in [49] [72] [45]. Table 4.1 shows the computational costs comparison among the schemes. Where t_p, t_1, t_2 denote as the time consumption of pairing, exponentiation in $\mathbb{G}_1$ and exponentiation in $\mathbb{G}_2$, respectively. On basis of the result of the running time as shown in Fig. 4.4, the proposed scheme have 9 exponentiation in G_1 and 3 pairing

operations when the sender A signcrypts the message and receiver B decrypts it. The running time is given as, $9 * 1.0 + 3 * 2.9 = 17.7\, ms$. Therefore, the time computation cost in the proposed scheme shows high efficiency and is much faster than the other schemes.

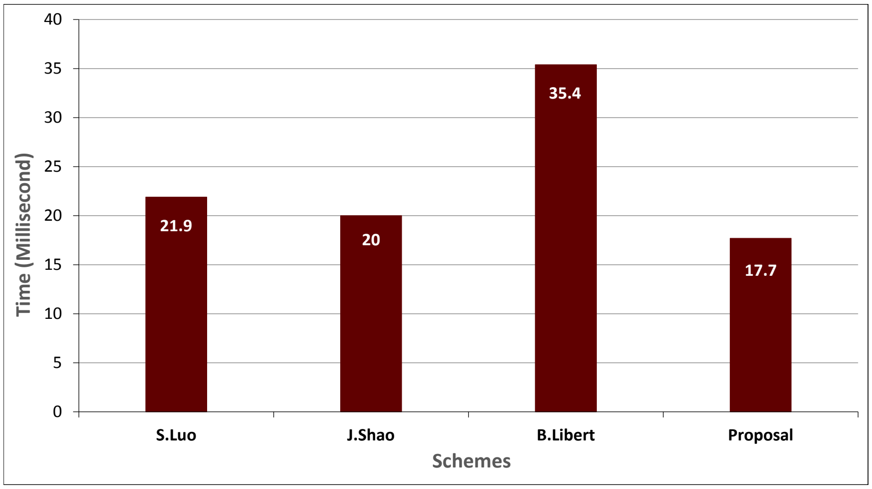

Figure 4.4: Efficiency comparison with other schemes.

b) In this case, a comparison is made between our scheme and other multiple receiver signcryption schemes in [83] [61] [98]. We mainly compare the computational cost at the signcryption operation phase. The proposed scheme, only takes $3t_1$ for signcrypting a message to one or even to number n receivers. This is because the sender signcrypts the message one time which is to himself, and then delegates a number of receivers to decrypt it by computing $U_j = (X_j^{v_i})_{j=1}^{n}$. As a result, the value of U_i will not affect the computation cost when the sender signcrypts the message. Fig. 4.5 shows the average computational delay between the proposed scheme and other existing schemes. The result shows that the scheme cannot be affected by increasing the number of the receivers compared to other schemes. Therefore, the computation cost is almost negligible in the proposed scheme and eliminates the issue of increased computation delay that most of multiple receiver signcryption schemes are suffering from, when the number of receivers are increased.

Table 4.2: Computational and communication overhead analysis.

Scheme	Communication Overhead	Time Signcryption
X.Wang [83]	$n(2+\|G_1\|+\|G_2\|+n\|ID'\|)+\|m\|$	n
B.Zhang [98]	$(2+2n)\|G_1\|+\|m\|+n\|ID'\|$	n
L.Pang [61]	$(2+2n)\|G_1\|+\|m\|+n\|ID\|$	n
proposed scheme	$(3+n)\|G_1\|+\|m\|$	1

To quantify the running time of the operations as displayed in table 4.3, we calculate the computation time for signcryption and unsigncryption by using an MNT curve. The curve's embedment degree is 6 and 160-bit q on an Intel Pentium IV 3.0 GHZ machine [66].

Table 4.3: Cryptographic operation running time.

	Descriptions	Execution Time
t_p	Pairing operation	2.9 ms
t_1	Exponentiation in G_1	1.0 ms
t_2	Exponentiation in G_2	0.2 ms

2. Communication Overhead.

The communication overhead determines the size of the ciphertext length. Since ciphertext size is an important factor affecting the efficiency, we present the comparison with respect to it. To make the comparison convincing, we compare the efficiency of our proposed scheme with existing proxy re-encryption schemes and multiple receiver signcryption schemes. In the proposed scheme the original ciphertext for one receiver is described as $\alpha_i = (E_i, F_i, \sigma_i, U_i)$. While the original ciphertext for n receivers is described as $\alpha_i = (E_i, F_i, \sigma_i, U_1, ..., U_n)$. Table 4.4 shows the communication overhead in our proposed scheme in terms of one receiver compared to proxy re-encryption schemes exists in [49] [72] [45]. While in table 4.2, we compare the communication overhead in our pro-

Table 4.4: Computational and communication overhead analysis

Scheme	Computational Cost	Communication Overhead
B.Libert [45]	$8t_1 + 4t_p + 2t_2$	$\|pk_s\| + 2\|G_1\| + \|G_2\| + \|\sigma_s\|$
J.Shao [72]	$6t_1 + 10t_p + 2t_2$	$3\|G_1\| + \|G_2\|$
S.Luo [49]	$7t_1 + 5t_p + 2t_2$	$3\|G_1\| + \|G_2\|$
Proposed scheme	$9t_1 + 3t_p$	$3\|G_1\| + \|m\|$

posed scheme with the multiple receivers signcryption schemes in [83] [61] [98] in terms of n of receivers. Thus, we can see that we have an efficient scheme that has much lower computational time, with reducing the communication overhead.

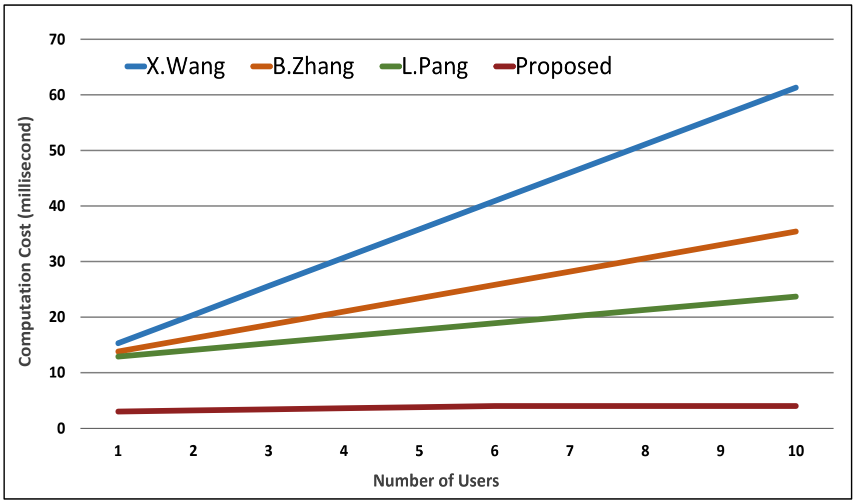

Figure 4.5: Efficiency comparison with other schemes

4.8 Conclusion

In this chapter, we have proposed a novel privacy-preserving mechanism to secure the task announcement in VCC system. In this mechanism, the VCC server signcrypts the task in order to conceal the task's content from any adversary or malicious RSU. The RSU re-signcrypts the message without knowing the content of this task or even destination. The proposed scheme combines the proxy re-encryption algorithm with the multiple receiver signcryption scheme in order to eliminate the increasing of computation cost when the number of receivers increase. Through performance analysis, we demonstrated the effectiveness of the proposed scheme in terms of the computational overhead and ciphertext size. The security analysis shows that the proposed scheme can resist various security threats in task announcement in the VCC system.

Chapter 5

Location Privacy-Aware Task Recommendation for Spatial Crowdsourcing

5.1 Introduction

Spatial Crowdsourcing [17] is a compelling paradigm that engages individuals in collecting, processing and analyzing data about environmental phenomena, social events, and other spatio-temporal information. With spatial crowdsourcing, customers outsource their spatial tasks to a group of workers, i.e., mobile users that collect data from specific regions using their devices [100]. Typically, a spatial crowdsourcing server (SC-server) acts as a broker between customers and workers to recruit workers for task fulfillment, and the workers participate in spatial crowdsourcing activities voluntarily or motivated by benefits. As this human-centric problem-solving paradigm is highly flexible, it can significantly reduce the cost and shorten the time on task accomplishment. Furthermore, with human intelligence, spatial crowdsourcing can improve the quality of task completion, such as translation and labelling. Currently, spatial crowdsourcing supports numerous applications in domains (e.g., journalism, environmental sensing, crisis response and urban planning).

Unlike traditional company, in which the tasks are accomplished by fix employees, spatial crowdsourcing recruits a set of workers from Internet to perform. Thus, this paradigm is feasible only if workers and tasks are matched effectively on both time and locations [82]. For example, to measure the traffic congestion in downtown Toronto at the morning peak hours, the SC-server should assign tasks to the workers driving on the roads in downtown Toronto at those hours. Otherwise, the workers have to pay extra costs on travelling and time to reach the required locations for task performing, which may discourage workers to participate in spatial crowdsourcing activities. Therefore, it is necessary for the SC-server to take into account the workers' locations when allocating spatial tasks. However, the SC-server may not be fully trusted, and the disclosure of individual locations has serious privacy implications from the perspective of workers. It is possible for attackers to predict the trajectory and living habit of a specific worker [64]. Protecting location privacy is essential in spatial crowdsourcing, as the workers may refuse to engage in spatial tasks if their privacy is invaded. To preserve worker's location privacy on task recommendation, many solutions have been proposed based on mix network, anonymity techniques and location differential privacy in spatial crowdsourcing. Unfortunately, these techniques have their inherit drawbacks. Specifically, mix network is built on the assumption that at least one of the network nodes is not compromised; the anonymity techniques, such as pseudonyms, blind signatures and group signatures, require either pseudonyms management or complex zero-knowledge proof to protect the workers' identities; and the location differential privacy sacrifices the accuracy of location matching to ensure the location privacy. Therefore, exploiting new approaches to preserve the location privacy for workers still deserves to may more efforts.

Even if the location privacy leakage is prevented, the crowdsourcing reports may still expose location information about customers [55]. For instances, from photos, videos and other spatial data, the attackers can know the places these photos and videos are taken and spatial data are collected, and thereby learn the locations of data sources. As a result, the location privacy of workers is violated. Moreover, the exposure of crowdsourcing reports might leak other personal information about workers, such as identities, occupations, references, home addresses, social relations, health status, and political ideology, which may cause plenty of troubles in daily life, e.g., malicious advertisements and harassing phone calls, even result in economic loss. In addition, the spatial tasks would expose the points of interest of customers, and their intension to release these tasks. In short, preserving crowdsourcing reports and spatial tasks are quite vital for workers in spatial crowdsourcing.

In this chapter, we propose a location privacy-aware task recommendation framework, called LATE, to protect the workers' locations during task recommendation in spatial crowdsourcing. By leveraging Lagrange Interpolating Polynomials, we achieve the privacy-preserving matching between the locations of workers and the geocast areas of spatial tasks in LATE. Specifically, the main contributions are as follows:

- A privacy-preserving location matching mechanism is designed from Lagrange Interpolating Polynomials. The geocast region of the spatial task is encrypted using a temperate public key and a searchable tag is generated from the worker's location and the corresponding temperate secret key. Having the ciphertext and tag, anyone can test whether the worker's location is one of the places in the geocast region.

- By leveraging the designed privacy-preserving location mechanism, LATE achieves secure spatial task recommendation with location privacy preservation for workers. The SC-server cannot know the geocast regions of spatial tasks and geographic locations of workers, but is enabled to determine whether the workers are located in the geocast regions of spatial tasks. Thereby, the SC-server can recommend the spatial tasks to the workers for fulfillment. In addition, we utilize a proxy re-encryption to encrypt the spatial tasks and crowdsourcing reports to prevent privacy leakage for both customers and workers.

- We prove the security of LATE to show that no attacker can learn anything about the locations of workers and the geocast areas of spatial tasks, and demonstrate the LATE is efficient and practical in terms of computational and communication overhead.

The remainder of the chapter is organised as follows. We first define the system model, threat model and design goals in Section 5.2. Then, we describe the LATE framework in Section 5.3 and discuss its security in Section 5.4, followed by the performance evaluation in Section 5.5. Finally, we conclude our work in Section 5.6.

5.2 Problem Statement

In this section, we define system models and security threats, and identify the design goals.

5.2.1 System Model

The spatial crowdsourcing system provides a people-centric approach to customers for data collection and analysis. As shown in Fig. 5.1, the architecture consists of four entities: a SC-server, a trust management server, customers and workers.

SC-Server: The SC-server offers spatial crowdsourcing services to customers. It has sufficient storage space, computational capability and communication bandwidth. It is responsible to receive spatial tasks from customers, recommend tasks to workers and collect the crowdsourcing reports to fulfill the tasks for customers.

Trust Management Server: The trust management server aims to manage the trust levels of all workers. It keeps the trust levels or reputations of workers and enables the SC-server to check whether the participating worker is honest to perform the recommended spatial tasks.

Customers: The customers can be individuals, corporations or organizations. They have some spatial tasks to accomplish, but they are unwilling to perform by themselves, and thereby they outsource their tasks on the SC-server and recruit workers to fulfill for them.

Workers: Each worker has the devices to perform the spatial tasks, e.g., smart phones, tablets, vehicles, computers and other items with sensors, computational units and storage spaces. These devices are carried by their owners wherever they go and whatever they do. The workers also make sure the sufficient power on devices to support their functions. With the devices, the workers can participate in spatial tasks by collecting data from environment, analyze data, process images and upload the reports to the SC server.

5.2.2 Security Threats

The spatial crowdsourcing system is confronted with serious security threats from both external and internal attackers. Specifically, the external attackers, e.g., eavesdroppers and hackers, wiretap on wireless communication channels to capture the messages exchanged between workers and SC-servers, and attack the servers or devices to obtain the administration rights. The internal adversaries include the SC-server and workers. The SC-server is honest to offer spatial crowdsourcing service to customers, but it may be curious on the workers. It may strive to know the spatia-temporal probability distribution for a specific worker and other sensitive information about workers and customers, e.g., preference, social relation, political affiliation and purchase intention, from the maintained information, including spatial tasks and crowdsourcing reports. The workers also try to learn sensitive information about the customers and the other workers. Specifically, they are willing to know the other workers participating in the same tasks, and learn more knowledge about customers to reach their expectancy. The geographic locations are extracted from Google Maps or GPS trusted chip on devices, modifying the locations for workers is infeasible. The trust management server is protected by trusted components and it is fully

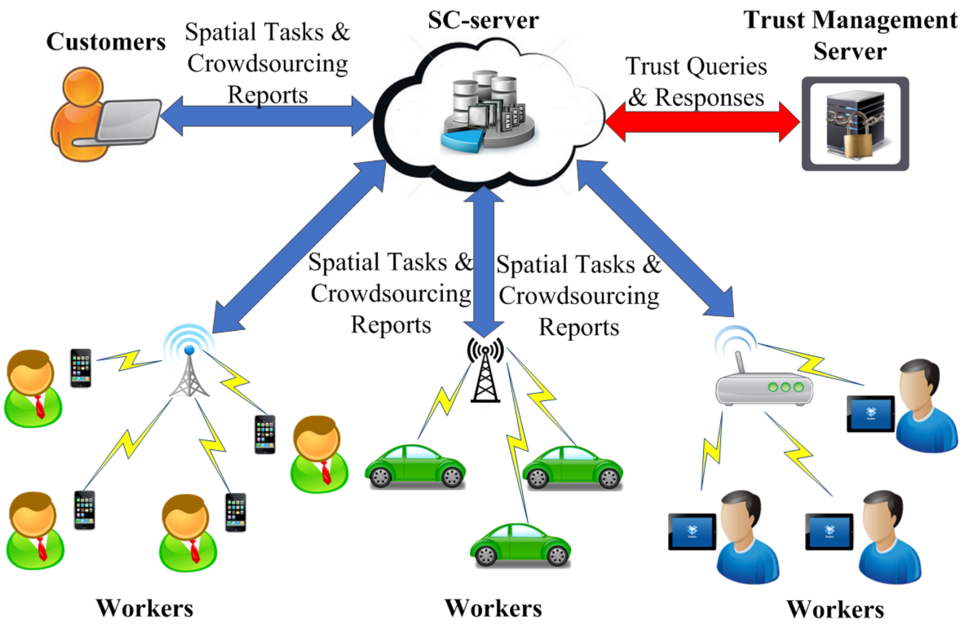
Customers
Spatial Tasks & Crowdsourcing Reports
SC-server
Trust Management Server
Trust Queries & Responses
Spatial Tasks & Crowdsourcing Reports
Spatial Tasks & Crowdsourcing Reports
Workers
Workers
Workers

Figure 5.1: System Model.

trusted by customers, workers and the SC-server. The customers are honest as well, since, being the beneficiaries, they have no incentives to disrupt the spatial crowdsourcing service.

5.2.3 Design Goals

To enable location privacy-aware task recommendation under the aforementioned system model and resist security threats, the LATE should achieve the following design goals:

- Task Recommendation: The spatial tasks should be recommended to the workers located in the geocast regions of spatial tasks to reduce the travel cost and time on task fulfillment, and the other workers outside the geocast regions should not learn any knowledge about the spatial tasks, even it they can obtain the encrypted spatial tasks.
- Location Privacy Preservation: The geographic locations of workers and the geocast regions of tasks are protected against malicious attackers and curious entities. The SC-server or a worker is only aware whether the geographical position is in the geocast area or not.

- Data Confidentiality: The crowdsourcing reports can only be accessed by the delegated customers, such that the privacy of workers would not be exposed to others.

5.3 The LATE Protocol

In this section, we propose the LATE protocol consisting of four phases, Service Setup, Task Releasing, Task Recommendation and Task Fulfillment. We first review the preliminaries, which is the basis of the LATE protocol.

5.3.1 Preliminaries

Lagrange Interpolating Polynomial Theorem [23]: Let $F(x) = \sum_{i=0}^{n} y_i f_i(x) = \sum_{i=0}^{n-1} a_i x^i$ be a polynomial of degree $n-1 \geq 0$ that passes through n points $(x_1, y_1), \cdots, (x_n, y_n)$ where for each i,

$$\begin{aligned} f_i(x) &= \prod_{1 \leq j \neq i \leq n} \frac{x - x_j}{x_i - x_j} \\ &= \begin{cases} 1 \quad , & x = x_i. \\ 0 \quad , & x \in \{x_1, \cdots, x_n\} \setminus \{x_i\}. \end{cases} \end{aligned}$$

Bilinear Pairing: Suppose G be a cyclic additive group with a prime order q, and G_T be a cyclic multiplicative group of the same order q. P is a generator of G. The map $\hat{e} : G_1 \times G_1 \to G_2$ is an admissible bilinear pairing [10] if the following conditions hold:

1. Bilinearity: for all $a, b \in Z_q^*$, $\hat{e}(P, P)^{ab} = \hat{e}(aP, bP)$.
2. Non-degeneracy: $\hat{e}(P, P) \neq 1_{G_2}$.
3. Computability: there exists an efficient algorithm to compute $\hat{e}$.

Complexity assumption: The intractable mathematical problem and complexity assumption used are as follows.

Co-Decisional Bilinear Diffie-Hellman (Co-DBDH) problem [15]: Given $< P, aP, bP, Q, Z >$ for some $a, b \in Z_q^*$, $P, Q \in G$ and $Z \in G_T$, output "1" if $Z = \hat{e}(P, Q)^{ab}$ and "0", otherwise.

Definition 1. An algorithm $\mathcal{B}$ with an output $\beta \in \{0, 1\}$ has an advantage ε in solving the Co-DBDH problem that $|\ \Pr[\mathcal{B}(P, aP, bP, Q, \hat{e}(P, Q)^{ab}) = 1] - \Pr[\mathcal{B}(P, aP, bP, Q, Z) = 1]\ | \geq \varepsilon$ where a, b are randomly from Z_q^* and Z is a random element from G_T.

The (τ, ε)-Co-DBDH assumption holds if no polynomial-time algorithm has an advantage ε within running time τ in solving the Co-DBDH problem.

5.3.2 The Detailed LATE

To achieve privacy-aware task recommendation, we uniquely utilize the Lagrange Interpolating Polynomials to design the location matching in LATE. We allow the SC-server to check whether the locations of workers are in the geocast areas of spatial tasks, without exposing the users' locations and geocast areas. In fact, the public key encryption with keyword search scheme [96] can be utilized to achieve the privacy-preserving matching for workers. Specifically, the geocast areas of spatial tasks are represented as a vector $L = \{l_1, l_2, \cdots, l_n\}$, and the location of a worker U is supported to be l. The SC-server can learn whether $l \in L$ with no knowledge about l and L. Thus, the SC-server can recommend the task with L to U, if $l \in L$. The detailed construction of LATE is described below.

Service Setup

The SC-server bootstraps the whole service and setups the system parameters. It chooses a security parameter k, which ensures the security level of the system and determines the prime order q of the bilinear groups. In general, $k = 256$ or 160. Let G be an additive cyclic group with a generator P and G_T be a multiplicative cyclic group equipped with q. $\hat{e}$ is a bilinear map $\hat{e} : G \times G \rightarrow G_T$. The service provider picks a random $Q \in G_1$ and two collision resistant hash functions $H_1 : \{0, 1\}^* \rightarrow Z_q^*$ and $H_2 : \{0, 1\}^* \rightarrow G_1$. $C = E_{AES}(K, M)$ and $M = D_{AES}(K, C)$ are the encryption and decryption algorithm of AES. The public parameter is $gp = \{q, G_1, G_2, \hat{e}, P, Q, H_1, H_2\}$. Besides, the SC-server initializes the service geographic regions for customers by defining the points of interest in the regions, such as shopping malls, plazas, museums and buildings.

A worker $\mathbb{U}$ is required to generate a public-private key pair (pk, sk) by picking a random $s \in Z_q^*$ to compute $P_{pub} = sP$. The public key is P_{pub}, while the private key is s. The certificate authority (CA) in public key infrastructure (PKI) issues and signs the certificate $cert_u$ for U, which includes series number, P_{pub}, signature algorithm, and signature, etc. The certificate is allowed the public to check the validity of $\mathbb{U}$'s public key, and $\mathbb{U}$'s secret key is kept on a Memory Protection Unit (MPU) to restrict access.

A customer $\mathbb{C}$ randomly chooses $v \in Z_q^*$ as the secret key and computes the public key as $V_{pub} = vP$. The CA also generates and issues a certificate $cert_c$ for $\mathbb{C}$. $\mathbb{C}$ keeps its secret key a MPU to restrict publicly access.

The trust management server (TMS) initializes its service for trust management for workers. It maintains a list L_M to record the trust level for each worker. TMS randomly picks $t \in Z_q^*$ as the secret key and calculates the public key as $T_{pub} = tP$. The CA also generates and issues a certificate $cert_t$ for TMS. TMS keeps its secret key on a MPU.

Task Releasing

When the customer $\mathbb{C}$ is willing to fulfill spatial crowdsourcing, it generates a spatial task $ST = (Cont, Expt, L)$, which indicates the content (what to sense), the expiration time (when to sense), the geocast area (where to sense). Other attributes (e.g., reporting interval, benefits, reporting periods) can be illustrated in $Cont$. $\mathbb{C}$ picks a random number num as the identifier. The geocast area L is denoted as $L = \{l_1, l_2, \cdots, l_n\}$, in which $l_i \in L$ a set of points of interest from which $\mathbb{C}$ needs to collect and analyze data. To prevent the exposure of geocast area $L = \{l_1, l_2, \cdots, l_n\}$, $\mathbb{C}$ generates a series of encrypted points of interest in the following way:

1. Pick a random value $k \in Z_q^*$ as the temperate secret key and compute the corresponding temperate public key $K_{pub} = kP$.
2. Pick a random value $\gamma \in Z_q^*$ to compute,
   - $C_1 = \gamma P$, and
   - $h = H_1(num, cert_c, \hat{e}(K_{pub}, \gamma Q))$.

3. For $i = \{1, \cdots, n\}$, compute, $x_i = H_1(l_i)$, and

$$\begin{aligned} f_i(x) &= \prod_{1 \leq j \neq i \leq n} \frac{x - x_j}{x_i - x_j} \\ &= a_{i,1} + a_{i,2}x + \cdots + a_{i,n}x^{n-1}. \end{aligned}$$

   where $a_{i,1}, \cdots, a_{i,n} \in Z_p^*$.

4. For $i = \{1, \cdots, n\}$, randomly pick $\alpha_i \in Z_q^*$, and calculate,
   - $y_i = \alpha_i^{-1}\gamma$
   - $U_i = \sum_{j=1}^{n} a_{j,i}\alpha_j K_{pub}$.
5. For $i = \{1, \cdots, n\}$, compute,
   - $X_i = H_2(l_i \mid\mid num)$
   - $R_i = \sum_{j=1}^{n} a_{j,i}y_j X_j$.
6. Set the ciphertexts of geocast area of $L = \{l_1, l_2, \cdots, l_n\}$ as,

$$C = (R_1, \cdots, R_n, U_1, \cdots, U_n, C_1, h).$$

Further, to prevent the task exposure, $\mathbb{C}$ utilizes TMS's public key to encrypt $Cont$, that is, picks a random value $w \in Z_q^*$, $Z \in G_T$ and computes,

- $D_0 = E_{AES}(H_1(num, Z), Cont)$,
- $D_1 = wtP$,
- $D_2 = Z \oplus \hat{e}(P, P)^w$.

After that, $\mathbb{C}$ also utilizes the TMS's public key T_{pub} to encrypt the temperate secret key k by randomly choosing $r \in Z_q^*$, $Y \in G_T$ to compute,

- $E_0 = E_{AES}(H_1(num, Y), k)$,

- $E_1 = trP$,
- $E_2 = Y \oplus \hat{e}(P, P)^r$.

Finally, $\mathbb{C}$ sends the encrypted spatial task $\mathcal{T} = (num, Expt, C, D_0, D_1, D_2, E_0, E_1, E_2)$ to the SC-server, and the SC-server releases $\mathcal{T}$ on its website.

Task Recommendation

When the worker $\mathbb{U}$ wants to participate in spatial crowdsourcing activities, $\mathbb{U}$ performs the following interactions with TMS and SC-server to retrieve the recommended spatial task:

1. $\mathbb{U}$ forwards $cert_u$ to the TMS.
2. The TMS checks $\mathbb{U}$'s trust level in L_M. If $\mathbb{U}$ is trusted, the TMS computes $E = \hat{e}(E_1, P_{pub})^{t^{-1}}$ and returns $(cert_t, E)$ to $\mathbb{U}$.
3. $\mathbb{U}$ utilizes its secret key s to decrypt (E, E_0, E_2) as,
   - $Y = E_2 \oplus E^{s^{-1}}$,
   - $k = D_{AES}(H_1(num, Y), E_0)$
4. $\mathbb{U}$ uses the location l to compute a location trapdoor $T_l = (T_1, T_2)$ as
   - $T_1 = H_1(l)$,
   - $T_2 = k(Q + H_2(l \mid\mid num))$.

   Then, $\mathbb{U}$ sends $(cert_u, T_l)$ to the SC-server.
5. The SC-server uses T_l to compute

$$\lambda = R_1 + R_2 T_1 + \cdots + R_n T_1^{n-1} \pmod q,$$

$$\nu = U_1 + U_2 T_1 + \cdots + U_n T_1^{n-1} \pmod q$$

and then checks whether

$$h \overset{?}{=} H_1(num, cert_c, \frac{\hat{e}(C_1, T_2)}{\hat{e}(\nu, \lambda)}). \tag{5.1}$$

If the equation (1) holds, which means that $\mathbb{U}$'s location l is in the geocast area L, the SC-server returns $(num, cert_u, D_0, D_1, D_2, Expt)$ to the TMS; otherwise, it returns failure to $\mathbb{U}$ and aborts.

6. The TMS re-encrypts the ciphertext of $Cont$ to be decryptable for $\mathbb{U}$ as, $D = \hat{e}(D_1, P_{pub})^{t^{-1}}$ and sends $(num, cert_u, D_0, D, D_2, Expt)$ to $\mathbb{U}$.
7. $\mathbb{U}$ utilizes its secret key s to decrypt (D, D_0, D_2) as,
   - $Z = D_2 \oplus D^{s^{-1}}$,
   - $Cont = D_{AES}(H_1(num, Z), D_0)$.

Finally, $\mathbb{U}$ obtains the content of task ST and performs the task if ST is not expired.

Task Fulfillment

$\mathbb{U}$ performs the spatial task ST and generates a crowdsourcing report R_c. To protect R_c, $\mathbb{U}$ uses $\mathbb{C}$'s public key V_{pub} to encrypt R_c using AES to generate a ciphertext F_c and sends $(num, cert_u, F_c)$ to $\mathbb{C}$. Finally, $\mathbb{C}$ decrypts F_c to recover $\mathbb{U}$'s report R_c and fulfills the spatial task ST according to the crowdsourcing reports from workers.

5.3.3 Correctness of LATE

Suppose $l \in L = \{l_1, l_2 \cdots, l_n\})$ without loss of generality, the correctness of task recommendation can be justified as follows:

$$\begin{array}{rcl}
\lambda & = & R_1 + \cdots + R_i T_1^{i-1} + \cdots + R_n T_1^{n-1} \\
& = & a_{1,1} y_1 X_1 + \cdots + a_{n,1} y_n X_n + \cdots \\
& + & a_{1,i} y_1 X_1 T_1^{i-1} + \cdots + a_{n,i} y_n X_n T_1^{i-1} + \cdots \\
& + & a_{1,n} y_1 X_1 T_1^{n-1} + \cdots + a_{n,n} y_n X_n T_1^{n-1} \\
& = & (a_{1,1} + \cdots + a_{1,n} T_1^{n-1}) y_1 X_1 + \cdots \\
& + & (a_{i,1} + \cdots + a_{i,n} T_1^{n-1}) y_i X_i + \cdots \\
& + & (a_{n,1} + \cdots + a_{n,n} T_1^{n-1}) y_n X_n \\
& = & y_i X_i
\end{array}$$

$$\begin{array}{rcl}
\nu & = & U_1 + \cdots + U_n T_1^{n-1} \\
& = & (a_{1,1} + \cdots + a_{1,n} T_1^{n-1}) \alpha_1 K_{pub} + \cdots \\
& + & (a_{i,1} + \cdots + a_{i,n} T_1^{n-1}) \alpha_i K_{pub} + \cdots \\
& + & (a_{n,1} + \cdots + a_{n,n} T_1^{n-1}) \alpha_n K_{pub} \\
& = & \alpha_i K_{pub}.
\end{array}$$

Thus,

$$\begin{array}{rcl}
\dfrac{\hat{e}(C_1, T_2)}{\hat{e}(\nu, \lambda)} & = & \dfrac{\hat{e}(\gamma P, k(Q + H_2(l \mid\mid num)))}{\hat{e}(\alpha_i K_{pub}, y_i X_i)} \\
& = & \dfrac{\hat{e}(\gamma P, (kQ + kH_2(l \mid\mid num)))}{\hat{e}(\alpha_i K_{pub}, y_i X_i)} \\
& = & \dfrac{\hat{e}(\gamma P, kQ)\hat{e}(\gamma P, kH_2(l \mid\mid num))}{\hat{e}(\alpha_i K_{pub}, \alpha_i^{-1} \gamma X_i)} \\
& = & \dfrac{\hat{e}(\gamma P, kQ)\hat{e}(\gamma P, kX_i)}{\hat{e}(kP, \gamma X_i)} \\
& = & \dfrac{\hat{e}(kP, \gamma Q)\hat{e}(\gamma P, kX_i)}{\hat{e}(\gamma P, kX_i)} \\
& = & \hat{e}(kP, Q)^{\gamma}.
\end{array}$$

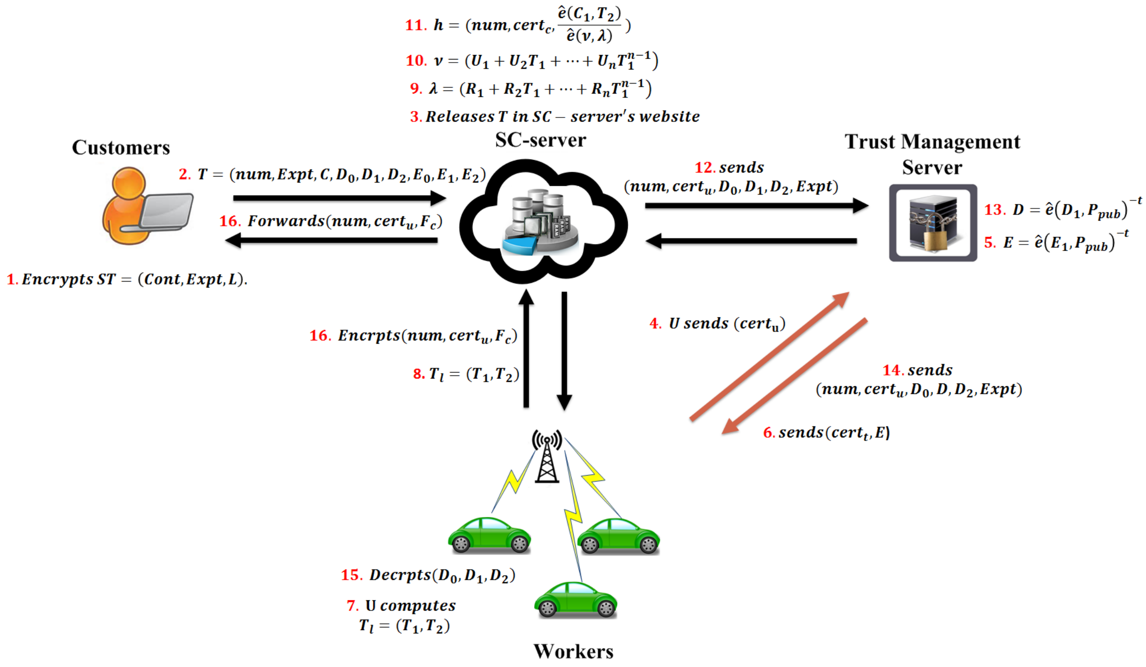
11. $h = (num, cert_c, \frac{\hat{e}(C_1, T_2)}{\hat{e}(\nu, \lambda)})$
10. $\nu = (U_1 + U_2T_1 + \cdots + U_nT_1^{n-1})$
9. $\lambda = (R_1 + R_2T_1 + \cdots + R_nT_1^{n-1})$
3. Releases T in $SC - server's$ website
Customers
SC-server
Trust Management Server
2. $T = (num, Expt, C, D_0, D_1, D_2, E_0, E_1, E_2)$
16. $Forwards(num, cert_u, F_c)$
12. sends $(num, cert_u, D_0, D_1, D_2, Expt)$
13. $D = \hat{e}(D_1, P_{pub})^{-t}$
5. $E = \hat{e}(E_1, P_{pub})^{-t}$
1. Encrypts $ST = (Cont, Expt, L)$.
4. U sends $(cert_u)$
16. $Encrpts(num, cert_u, F_c)$
8. $T_l = (T_1, T_2)$
14. sends $(num, cert_u, D_0, D, D_2, Expt)$
6. $sends(cert_t, E)$
15. $Decrpts(D_0, D_1, D_2)$
7. U computes $T_l = (T_1, T_2)$
Workers

Figure 5.2: Location privacy-aware task recommendation.

5.4 Security Discussion

In this section, we discuss the confidentiality of the workers' locations and crowdsourcing reports in LATE.

The goal of location privacy is to protect the workers' locations from being known by others. To protect the workers' locations, it is necessary to preserve the geocast areas of spatial tasks, since anyone can detect whether a worker's location is in the public geocast areas. Therefore, the confidentiality of geocast areas is critical for the protection of workers' locations. Thereby, the location privacy can be divided into two parts: geocast area privacy and worker's location privacy. The geocast area L is encrypted by a temperate public key K_{pub} to generate $C = (R_1, \cdots, R_n, U_1, \cdots, U_n, C_1, h)$. If there exists an adversary $\mathcal{A}$ who can identify the points of interest in L, there exists another algorithm $\mathcal{C}$ who can use $\mathcal{A}$ to solve an instance of the Co-DBDH problem, that is, given $(P, u_1 = aP, u_2 = bP, Q, Z \in G_2)$, its goal is to tell whether $Z = \hat{e}(P, Q)^{ab}$. We employee a simulator $\mathcal{C}$ to interact with $\mathcal{A}$ to prove the indistinguishability of the points of interest in L. To prove that, $\mathcal{C}$ setups the system by defining the public parameters

$(q, G, G_T, \hat{e}, P, Q, K_{pub}, H_1, H_2)$, in which $P_{pub} = u_2$ and H_1, H_2 are random oracles, and sends the public parameters to $\mathcal{A}$. $\mathcal{C}$ can answer the H_1-queries, H_2-queries and trapdoor queries from $\mathcal{A}$. $\mathcal{A}$ produces two points of interest l_0^* and l_1^*, and generates the ciphertext on one of them c_β^*, in which $\beta \in \{0, 1\}$. Finally, if $\mathcal{A}$ outputs a correct guess $\beta' \in \{0, 1\}$ that $\beta' = \beta$, $\mathcal{C}$ can utilize the guess to solve an instance of the co-DBDH problem. Since the co-DBDH problem is intractable, it is impossible for $\mathcal{A}$ to distinguish the encrypted points of interest. Therefore, the LATE can achieve the confidentiality of geocast areas of spatial tasks. In terms of the secrecy of a worker's location l, it is hashed to generate the location trapdoor T_l. As the hash function is one-way, it is impossible for the adversary $\mathcal{A}$ to learn any knowledge about the worker's location, unless it tests all the locations to find the proper one.

The spatial tasks and crowdsourcing reports are encrypted using the proxy re-encryption scheme [6] to prevent malicious attackers, e.g., eavesdroppers, hackers, to learn the private information about the customers and workers. Specifically, the customer encrypts the spatial task using the public key T_{pub} of TMS and the TMS is able to transform the ciphertext of spatial task to be decryptable for the recommended workers. Similarly, the worker utilizes the public key of the customer V_{pub} to protect the crowdsourcing reports R_c. The confidentiality of spatial tasks directly depends on the sematic security of the proxy re-encryption scheme, which can be reduced to the simplified $q-$DBDHI assumption [6] and the secrecy of crowdsourcing reports can be reduced to the security of AES.

5.5 Performance Evaluation

To demonstrate the computational overhead of LATE, we count the number of complicate cryptographic operations, including scalar multiplication in G, multiplication in G_T, the exponentiation in G_T and the bilinear pairing. We denote by SM_G, Mul_{G_T}, Exp_{G_T} and BP, the point multiplication in G_1, multiplication in G_2, the exponentiation in G_2 and the pairing computation. We also execute our proposed LATE on a notebook with Intel Core i5-4200U CPU @2.29GHz and 4.00GB memory. We use MIRACL library 5.6.1 to implement number-theoretic based methods of cryptography. The Weil pairing is utilized to realize the bilinear pairing operation. To ensure the security of the LATE, the parameter q is approximately 160 bits and the elliptic curve is defined as $y = x^3 + 1$ over $\mathbb{F}_p$, where p is 512 bits. The number of complicate cryptographic operations and the run time of each phase in LATE are in Table 5.1.

Table 5.1: Computational overhead of LATE.

Phases	**Operations**	**Run Time (ms)**
Setup	$3SM_G$	17.4
Releasing	$(2n+4)SM_G + 3Exp_{G_T} + 3BP$	185.4
Recommendation	$(2n-1)SM_G + Mul_{G_T}$ $+4Exp_{G_T} + 4P$	206.9
Fulfillment	0	10.5

We also analyze the communication overhead of LATE. When a customer outsources a spatial task, it needs to send the encrypted spatial task T to the SC-server, which is 4864+1024n bits, if we assume the binary length of $Expt$, $Cont$ and num is 256 bits. A worker also sends its $(cert_c, T_l)$ to the SC-server and receives the recommended spatial task. In Fig. 5.3, we show the binary length of the encrypted spatial task with respect to the number of location in the geocast region of a spatial area. The binary length of the encrypted spatial task increases linearly with the growth of n.

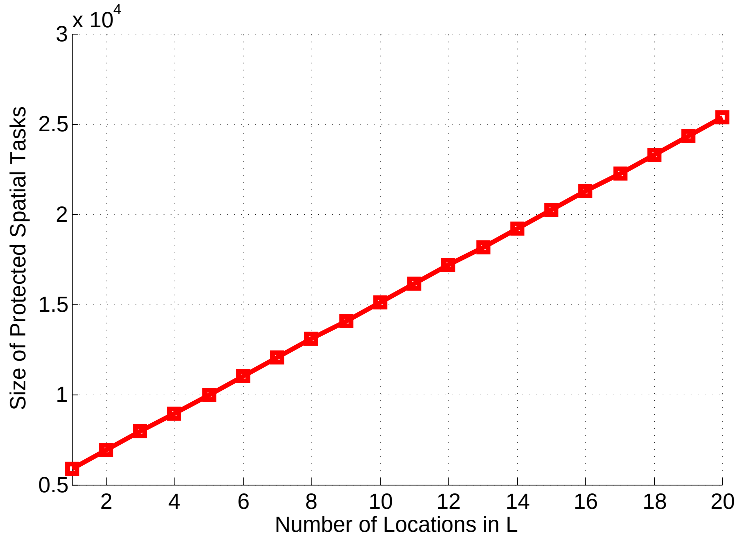

Figure 5.3: Communication Overhead.

5.6 Conclusions

In this chapter, we proposed a location privacy-aware task recommendation framework to protect the location privacy for workers during task recommendation in spatial crowdsourcing. Specifically, we have designed a privacy-preserving location matching mechanism to enable the SC-server to determine whether the workers are located in the geographic areas of spatial tasks without learning any information about workers' locations. Thus, the SC-server is able to recommend the spatial tasks to the workers in the geocast regions for fulfillment, and it is unnecessary for the workers to travel to specific regions to perform the spatial tasks for customers. Thereby, the cost on travel and time for workers are reduced. In addition, the spatial tasks and crowdsourcing reports are encrypted during transmission to prevent workers' privacy leakage from them.

Chapter 6

Conclusions and Future Work

In this chapter, we summarize our contributions in this thesis and propose future research.

6.1 Contributions

The major contributions of this thesis can be summarized as follows:

- First, we propose a tendering-based incentive framework for encouraging vehicles to participate using their onboard capabilities in the VCC system. Due to fact that modern vehicles have a variety of resources, they can be selected by the VCC server as resource providers. In order to ensure the fairness among vehicles, we introduce an illustrative language that is capable of describing heterogeneous vehicular resource types as a novel approach. In addition, we exploit game theory in order to design a *truthful privacy preserving tendering (TPPT) mechanism* that ensures truthful tenders and helps the VCC server to select the vehicle with optimal resources for the task. The signcryption technique with the homomorphic concept is used in this work to preserve the truthful information reported by vehicles from being disclosed. The proposed TPPT scheme is much more efficient and guarantees the truthful tenders compared with the other popular game theory schemes applied in VCC [20] [91] [92]. Also, it has been found that, in terms of the communication and computational overheads, the proposed scheme is significantly more efficient than the existing schemes.

- Second, due to fact that a vehicle's location privacy is likely to be disclosed during task announcement, we introduce a new mechanism called MRPRS, which stands for multiple receiver proxy re-signcryption technique. The proposed scheme combines the proxy re-encryption with multiple receiver signcryption in order to eliminate an increase in computational cost when the number of receivers increase. We use MRPRS as a concealing mechanism against disclosure of the vehicle's privacy during task announcement. The VCC server signcrypts the task in order to conceal the task content from any adversary or malicious RSU. The RSU re-signcrypts the message without knowing the content of this task or even the destination. MRPRS shows the efficiency in terms of computational costs and ciphertext size compared to the other multiple receiver signcryption schemes and proxy re-encryption schemes. The security analysis shows the MRPRS can resist various security threats in task announcement in the VCC system.

- Third, inspired by the fact that vehicles privacy can also be disclosed when a VCC server recommends suitable vehicles for spatial tasks, we propose a novel location privacy-awareness task recommendation framework (LATE) in spatial crowdsourcing. The proposed scheme enables the VCC server to recommend spatial tasks to the vehicles in geocast regions of spatial tasks. The geocast regions of spatial tasks and geographical location of vehicles cannot be known by the VCC server. However, it can determine whether the vehicles are located in the geocast regions of spatial tasks. Proxy re-encryptions is used in order to encrypt vehicle reports and spatial tasks so as to avoid leakage of privacy for both customers and vehicles. The security analysis proves that the attacker is unable to learn anything about the locations of vehicles or even the geocast areas of spatial tasks. In addition, we demonstrate that LATE is efficient and practical in terms of computational and communication overhead.

6.2 Future Work

In future work, we plan to carry out the developed framework with the automobile industry to build VCC applications in real world situations. In addition, the following research topics will be investigated as a continuation of my Ph.D. work.

- Vehicles in same location may generate identical sensing reports, which result in increased computational costs and communication overhead that lead to latency. To detect the redundant copies on intermediates, we need to inspect the report content. However, this solution will violate vehicle privacy. Using encryption methods can prevent the information from being disclosed, but the issue is how to detect the reduplicate data while they are encrypted.

- In modern vehicles, the OBU system is responsible for controlling and diagnosing onboard sensors as well as reporting any problems related to their functionality. However, the OBU system is considered an entry point to attack the vehicle functionality that may cause a big damage such as crashing vehicle. To realize the volume of the security threats confronting vehicles, it is important to know that all the sensor components associated with safety or non-safety in the vehicle are controlled by the OBU system. Thus, security threats may originate from connecting to the OBU system port. For example, when a third-party is physically connected to a vehicle's OBU system port or non-physically via Bluetooth or Wi-Fi for diagnostics purpose, it may set up of some auto mobile applications on the vehicle's OBU system. Malicious codes or viruses can be installed in the OBU system by these mobile applications that can leave the vehicle more vulnerable for attacks and result in affect the vehicle's functionality, for example, disabling the brakes or turning on all the lights in the vehicle to drain the battery.

While there is no general solution or scheme for a wide variety of many security and privacy issues in VCC, we plan to study cryptography and game theory more deeply to determine suitable and efficient schemes that can address the above challenges in a VCC paradigm.

Bibliography

[1] ABDELHAMID, S., HASSANEIN, H. S., AND TAKAHARA, G. Vehicle as a mobile sensor. *Procedia Computer Science 34* (2014), 286–295.

[2] ABDELHAMID, S., HASSANEIN, H. S., AND TAKAHARA, G. Vehicle as a resource (vaar). *IEEE Network 29*, 1 (2015), 12–17.

[3] AN, J., GUI, X., WANG, Z., YANG, J., AND HE, X. A crowdsourcing assignment model based on mobile crowd sensing in the internet of things. *IEEE Internet of Things Journal 2*, 5 (2015), 358–369.

[4] ARIF, S., OLARIU, S., WANG, J., AND KHALIL, I. Datacenter at the airport: Reasoning about time-dependent parking lot occupancy. *IEEE Trans. on Parallel and Distributed Syst. 23*, 11 (2012), 2067–2080.

[5] ARIF, S., OLARIU, S., WANG, J., YAN, G., YANG, W., AND KHALIL, I. Datacenter at the airport: Reasoning about time-dependent parking lot occupancy. *IEEE Transactions on Parallel and Distributed Systems 23*, 11 (2012), 2067–2080.

[6] ATENIESE, G., FU, K., GREEN, M., AND HOHENBERGER, S. Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Transactions on Information and System Security (TISSEC) 9*, 1 (2006), 1–30.

[7] BAO, F., AND DENG, R. H. A signcryption scheme with signature directly verifiable by public key. *International Workshop on Public Key Cryptography* (1998), 55–59.

[8] BELLARE, M., AND ROGAWAY, P. Random oracles are practical: A paradigm for designing efficient protocols. *Proceedings of the 1st ACM conference on Computer and communications security* (1993), 62–73.

[9] Blaze, M., Bleumer, G., and Strauss, M. Divertible protocols and atomic proxy cryptography. *Advances in CryptologyEUROCRYPT'98* (1998), 127–144.

[10] Boneh, D., and Franklin, M. Identity-based encryption from the weil pairing. *SIAM journal on computing 32*, 3 (2003), 586–615.

[11] Boneh, D., Gentry, C., Lynn, B., and Shacham, H. Aggregate and verifiably encrypted signatures from bilinear maps. *Advances in cryptologyEUROCRYPT 2003* (2003), 416–432.

[12] Boneh, D., Gentry, C., and Waters, B. Collusion resistant broadcast encryption with short ciphertexts and private keys. In *Crypto* (2005), vol. 3621, Springer, pp. 258–275.

[13] Boutsis, I., and Kalogeraki, V. On task assignment for real-time reliable crowdsourcing. In *Distributed Computing Systems (ICDCS), 2014 IEEE 34th International Conference on* (2014), IEEE, pp. 1–10.

[14] Buttyán, L., and Hubaux, J.-P. Stimulating cooperation in self-organizing mobile ad hoc networks. *Mobile Networks and Applications 8*, 5 (2003), 579–592.

[15] Chabanne, H., Phan, D. H., and Pointcheval, D. Public traceability in traitor tracing schemes. 542–558.

[16] Chen, T., Wu, L., Wu, F., and Zhong, S. Stimulating cooperation in vehicular ad hoc networks: a coalitional game theoretic approach. *IEEE Transactions on Vehicular Technology 60*, 2 (2011), 566–579.

[17] Chittilappilly, A. I., Chen, L., and Amer-Yahia, S. A survey of general-purpose crowdsourcing techniques. *IEEE Transactions on Knowledge and Data Engineering 28*, 9 (2016), 2246–2266.

[18] De Cristofaro, E., and Soriente, C. Extended capabilities for a privacy-enhanced participatory sensing infrastructure (pepsi). *IEEE Transactions on Information Forensics and Security 8*, 12 (2013), 2021–2033.

[19] Dimitriou, T., Krontiris, I., and Sabouri, A. Pepper: A querier's privacy enhancing protocol for participatory sensing. In *MobiSec* (2012), Springer, pp. 93–106.

[20] DUAN, L., KUBO, T., SUGIYAMA, K., HUANG, J., HASEGAWA, T., AND WALRAND, J. Incentive mechanisms for smartphone collaboration in data acquisition and distributed computing. *INFOCOM, 2012 Proceedings IEEE* (2012), 1701–1709.

[21] DUAN, S., AND CAO, Z. Efficient and provably secure multi-receiver identity-based signcryption. In *ACISP* (2006), vol. 6, Springer, pp. 195–206.

[22] ELTOWEISSY, M., OLARIU, S., AND YOUNIS, M. Towards autonomous vehicular clouds. *Ad hoc networks* (2010), 1–16.

[23] FAN, C.-I., HUANG, L.-Y., AND HO, P.-H. Anonymous multireceiver identity-based encryption. *IEEE Transactions on Computers 59*, 9 (2010), 1239–1249.

[24] FENG, Z., ZHU, Y., ZHANG, Q., NI, L. M., AND VASILAKOS, A. V. Trac: Truthful auction for location-aware collaborative sensing in mobile crowdsourcing. *IEEE INFOCOM* (2014), 1231–1239.

[25] FIAT, A., AND NAOR, M. Broadcast encryption. 480–491.

[26] FLEMING, W. J. New automotive sensors-a review. *IEEE Sensors Journal 8*, 11 (2008), 1900–1921.

[27] GENTRY, C. *A fully homomorphic encryption scheme*. PhD thesis, Stanford University, 2009.

[28] GENTRY, C., AND RAMZAN, Z. Identity-based aggregate signatures. In *Public Key Cryptography* (2006), vol. 3958, Springer, pp. 257–273.

[29] GERLA, M. Vehicular cloud computing. *Ad Hoc Networking Workshop (Med-Hoc-Net), 2012 The 11th Annual Mediterranean* (2012), 152–155.

[30] GIBBONS, R. *A primer in game theory*. Harvester Wheatsheaf, 1992.

[31] GUO, B., LIU, Y., WU, W., YU, Z., AND HAN, Q. Activecrowd: A framework for optimized multitask allocation in mobile crowdsensing systems. *IEEE Transactions on Human-Machine Systems 47*, 3 (2017), 392–403.

[32] HALEVY, D., AND SHAMIR, A. The lsd broadcast encryption scheme. *Advances in CryptologyCRYPTO 2002* (2002), 145–161.

[33] HAN, Y., LU, W., AND ZHANG, J. Identity based aggregate signcryption scheme. *Proceedings of the 9th International Symposium on Linear Drives for Industry Applications, Volume 4* (2014), 383–389.

[34] JIN, Z., WEN, Q., AND DU, H. An improved semantically-secure identity-based signcryption scheme in the standard model. *Computers & Electrical Engineering 36*, 3 (2010), 545–552.

[35] KLEMPERER, P. Auctions: theory and practice.

[36] LAFFONT, J.-J., AND MARTIMORT, D. *The theory of incentives: the principal-agent model*. Princeton university press, 2009.

[37] LAFFONT, J.-J., AND TIROLE, J. *A theory of incentives in procurement and regulation*. MIT press, 1993.

[38] LAL, S., AND KUSHWAH, P. Anonymous id based signcryption scheme for multiple receivers. *IACR Cryptology ePrint Archive 2009* (2009), 345.

[39] LEE, E., LEE, E.-K., GERLA, M., AND OH, S. Y. Vehicular cloud networking: architecture and design principles. *IEEE Communications Magazine 52*, 2 (2014), 148–155.

[40] LEE, S.-B., PAN, G., PARK, J.-S., GERLA, M., AND LU, S. Secure incentives for commercial ad dissemination in vehicular networks. *Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing* (2007), 150–159.

[41] LEE, U., AND GERLA, M. A survey of urban vehicular sensing platforms. *Computer Networks 54*, 4 (2010), 527–544.

[42] LEHMANN, D. Truth revelation in approximately efficient combinatorial auctions. *Journal of the ACM 49* (2002), 2002.

[43] LI, F., HU, Y., AND LIU, S. Efficient and provably secure multi-recipient signcryption from bilinear pairings. *Wuhan University Journal of Natural Sciences 12*, 1 (2007), 17–20.

[44] LI, F., AND WU, J. Frame: An innovative incentive scheme in vehicular networks. *2009 IEEE International Conference on Communications* (2009), 1–6.

[45] LIBERT, B., AND VERGNAUD, D. Unidirectional chosen-ciphertext secure proxy re-encryption. *IEEE Transactions on Information Theory 57*, 3 (2011), 1786–1802.

[46] LIM, K., AND ABUMUHFOUZ, I. M. Stors: secure token reward system for vehicular clouds. *SoutheastCon 2015* (2015), 1–2.

[47] LIM, K., ABUMUHFOUZ, I. M., AND MANIVANNAN, D. Secure incentive-based architecture for vehicular cloud. *Ad-hoc, Mobile, and Wireless Networks* (2015), 361–374.

[48] LIN, X., LU, R., ZHANG, C., ZHU, H., HO, P.-H., AND SHEN, X. Security in vehicular ad hoc networks. *IEEE communications magazine 46*, 4 (2008).

[49] LUO, S., SHEN, Q., AND CHEN, Z. Fully secure unidirectional identity-based proxy re-encryption. 109–126.

[50] MACHO-STADLER, I., AND PÉREZ-CASTRILLO, J. D. *An introduction to the economics of information: incentives and contracts.* Oxford University Press on Demand, 2001.

[51] MALONE-LEE, J. Identity-based signcryption. *IACR Cryptology ePrint Archive 2002* (2002), 98.

[52] MAMBO, M., AND OKAMOTO, E. Proxy cryptosystems: Delegation of the power to decrypt ciphertexts. *IEICE transactions on fundamentals of electronics, Communications and computer sciences 80*, 1 (1997), 54–63.

[53] MENEZES, A. J., VAN OORSCHOT, P. C., AND VANSTONE, S. A. *Handbook of applied cryptography.* CRC press, 1996.

[54] NASH, J. Non-cooperative games. *Annals of mathematics* (1951), 286–295.

[55] NI, J., LIN, X., ZHANG, K., AND YU, Y. Secure and deduplicated spatial crowdsourcing: A fog-based approach. In *Global Communications Conference (GLOBECOM), 2016 IEEE* (2016), IEEE, pp. 1–6.

[56] NI, J., ZHANG, K., LIN, X., XIA, Q., AND SHEN, X. S. Privacy-preserving mobile crowdsensing for located-based applications. In *Communications (ICC), 2017 IEEE International Conference on* (2017), IEEE, pp. 1–6.

[57] NISAN, N., ROUGHGARDEN, T., TARDOS, E., AND VAZIRANI, V. V. *Algorithmic game theory*. Cambridge University Press Cambridge, 2007.

[58] OGBURN, M., TURNER, C., AND DAHAL, P. Homomorphic encryption. *Procedia Computer Science 20* (2013), 502–509.

[59] OLARIU, S., ELTOWEISSY, M., AND YOUNIS, M. Towards autonomous vehicular clouds. *EAI Endorsed Trans. Mobile Communications Applications 1*, 1 (2011), e2.

[60] OLARIU, S., KHALIL, I., AND ABUELELA, M. Taking vanet to the clouds. *International Journal of Pervasive Computing and Communications 7*, 1 (2011), 7–21.

[61] PANG, L., LI, H., AND WANG, Y. nmibas: A novel multi-receiver id-based anonymous signcryption with decryption fairness. *Computing and Informatics 32*, 3 (2013), 441–460.

[62] POURNAJAF, L., GARCIA-ULLOA, D. A., XIONG, L., AND SUNDERAM, V. Participant privacy in mobile crowd sensing task management: a survey of methods and challenges. *ACM SIGMOD Record 44*, 4 (2016), 23–34.

[63] RAI, A., PADMANABHAN, V. N., AND SEN, R. Zee: zero-effort crowdsourcing for indoor localization. *ACM MobiCom* (2012), 293–304.

[64] REN, J., ZHANG, Y., ZHANG, K., AND SHEN, X. Exploiting mobile crowdsourcing for pervasive cloud services: challenges and solutions. *IEEE Communications Magazine 53*, 3 (2015), 98–105.

[65] SALANIÉ, B. *The economics of contracts: a primer*. MIT press, 2005.

[66] SCOTT, M. Efficient implementation of cryptographic pairings. *Online]. http://www. pairing-conference. org/2007/invited/Scott slide. pdf* (2007).

[67] SELVI, S. S. D., VIVEK, S. S., GOPALAKRISHNAN, R., KARUTURI, N. N., AND RANGAN, C. P. Provably secure id-based broadcast signcryption (ibbsc) scheme. *IACR Cryptology ePrint Archive 2008* (2008), 225.

[68] SELVI, S. S. D., VIVEK, S. S., SHRIRAM, J., KALAIVANI, S., AND RANGAN, C. P. Identity based aggregate signcryption schemes. *International Conference on Cryptology in India* (2009), 378–397.

[69] SELVI, S. S. D., VIVEK, S. S., SHRIRAM, J., KALAIVANI, S., AND RANGAN, C. P. Security analysis of aggregate signature and batch verification signature schemes. *IACR Cryptology ePrint Archive 2009* (2009), 290.

[70] SELVI, S. S. D., VIVEK, S. S., SHRIRAM, J., AND RANGAN, C. P. Efficient and provably secure identity based aggregate signature schemes with partial and full aggregation. *Cryptography ePrint Archive, Report 461* (2010), 2010.

[71] SEO, M., AND KIM, K. Electronic funds transfer protocol using domain-verifiable signcryption scheme. *International Conference on Information Security and Cryptology* (1999), 269–277.

[72] SHAO, J. Anonymous id-based proxy re-encryption. *Australasian Conference on Information Security and Privacy* (2012), 364–375.

[73] SHEN, Y., HUANG, L., LI, L., LU, X., WANG, S., AND YANG, W. Towards preserving worker location privacy in spatial crowdsourcing. In *Global Communications Conference (GLOBECOM), 2015 IEEE* (2015), IEEE, pp. 1–6.

[74] SHIN, M., CORNELIUS, C., PEEBLES, D., KAPADIA, A., KOTZ, D., AND TRIANDOPOULOS, N. Anonysense: A system for anonymous opportunistic sensing. *Pervasive and Mobile Computing 7*, 1 (2011), 16–30.

[75] SHIRAZ, M., GANI, A., KHOKHAR, R. H., AND BUYYA, R. A review on distributed application processing frameworks in smart mobile devices for mobile cloud computing. *IEEE Communications Surveys & Tutorials 15*, 3 (2013), 1294–1313.

[76] STACKELBERG, H. V., ET AL. Theory of the market economy.

[77] STALLINGS, W. *Cryptography and network security: principles and practices*. Pearson Education India, 2006.

[78] STANKOVÁ, K. *On Stackelberg and Inverse Stackelberg Games & Their Applications in the Optimal Toll Design Problem, the Energy Markets Liberalization Problem, and in the Theory of Incentives*. TU Delft, Delft University of Technology, 2009.

[79] TAN, C.-H. On the security of provably secure multi-receiver id-based signcryption scheme. *IEICE transactions on fundamentals of electronics, communications and computer sciences 91*, 7 (2008), 1836–1838.

[80] Thenmozhi, R., and Govindarajan, S. Safety related services using smart vehicle connections. *International Journal of Applied Engineering Research 11*, 4 (2016), 2384–2387.

[81] To, H., Ghinita, G., and Shahabi, C. A framework for protecting worker location privacy in spatial crowdsourcing. *Proceedings of the VLDB Endowment 7*, 10 (2014), 919–930.

[82] Wang, L., Zhang, D., Wang, Y., Chen, C., Han, X., and M'hamed, A. Sparse mobile crowdsensing: challenges and opportunities. *IEEE Communications Magazine 54*, 7 (2016), 161–167.

[83] Wang, X., Shu, J., Zheng, W., Liu, L., and Fan, X. New multi-receiver id-based ring signcryption scheme. *Unifying Electrical Engineering and Electronics Engineering* (2014), 2251–2257.

[84] Wang, Z., Wu, Q., Ye, D.-f., and Chen, H.-y. Practical identity-based aggregate signature from bilinear maps. *Journal of Shanghai Jiaotong University (Science) 13*, 6 (2008), 684–687.

[85] Wen, Y., and Ma, J. An aggregate signature scheme with constant pairing operations. In *Computer Science and Software Engineering, 2008 International Conference on* (2008), vol. 3, IEEE, pp. 830–833.

[86] Wen, Y., Shi, J., Zhang, Q., Tian, X., Huang, Z., Yu, H., Cheng, Y., and Shen, X. Quality-driven auction-based incentive mechanism for mobile crowd sensing. *IEEE Transactions on Vehicular Technology 64*, 9 (2015), 4203–4214.

[87] Whaiduzzaman, M., Sookhak, M., Gani, A., and Buyya, R. A survey on vehicular cloud computing. *Journal of Network and Computer Applications 40* (2014), 325–344.

[88] Xiao, M., Wu, J., Huang, L., Wang, Y., and Liu, C. Multi-task assignment for crowdsensing in mobile social networks. In *Computer Communications (INFOCOM), 2015 IEEE Conference on* (2015), IEEE, pp. 2227–2235.

[89] Xie, H., Kulik, L., and Tanin, E. Privacy-aware traffic monitoring. *IEEE Transactions on Intelligent Transportation Systems 11*, 1 (2010), 61–70.

[90] YAN, G., WEN, D., OLARIU, S., AND WEIGLE, M. C. Security challenges in vehicular cloud computing. *IEEE Transactions on Intelligent Transportation Systems 14*, 1 (2013), 284–294.

[91] YANG, D., XUE, G., FANG, X., AND TANG, J. Crowdsourcing to smartphones: incentive mechanism design for mobile phone sensing. *Proc. ACM MobiCom* (2012), 173–184.

[92] YANG, D., XUE, G., FANG, X., AND TANG, J. Incentive mechanisms for crowdsensing: Crowdsourcing with smartphones. *Biological Cybernetics 24*, 3 (2016), 1732–1744.

[93] YU, G., MA, X., SHEN, Y., AND HAN, W. Provable secure identity based generalized signcryption scheme. *Theoretical Computer Science 411*, 40 (2010), 3614–3624.

[94] YU, H., MIAO, C., SHEN, Z., LEUNG, C., CHEN, Y., AND YANG, Q. Efficient task sub-delegation for crowdsourcing. In *AAAI* (2015), pp. 1305–1312.

[95] YU, R., ZHANG, Y., GJESSING, S., XIA, W., AND YANG, K. Toward cloud-based vehicular networks with efficient resource management. *Network, IEEE 27*, 5 (2013), 48–55.

[96] YU, Y., NI, J., YANG, H., MU, Y., AND SUSILO, W. Efficient public key encryption with revocable keyword search. *Security and Communication Networks 7*, 2 (2014), 466–472.

[97] YU, Y., YANG, B., HUANG, X., AND ZHANG, M. Efficient identity-based signcryption scheme for multiple receivers. In *ATC* (2007), vol. 7, Springer, pp. 13–21.

[98] ZHANG, B., AND XU, Q. An id-based anonymous signcryption scheme for multiple receivers secure in the standard model. *Advances in Computer Science and Information Technology* (2010), 15–27.

[99] ZHANG, H., JIANG, H., LI, B., LIU, F., VASILAKOS, A. V., AND LIU, J. A framework for truthful online auctions in cloud computing with heterogeneous user demands. *IEEE Transactions on Computers 65*, 3 (2016), 805–818.

[100] ZHAO, Y., AND HAN, Q. Spatial crowdsourcing: current state and future directions. *IEEE Communications Magazine 54*, 7 (2016), 102–107.

[101] ZHENG, Y. Digital signcryption or how to achieve cost (signature & encryption)ł cost (signature)+ cost (encryption). *Annual International Cryptology Conference* (1997), 165–179.

[102] ZHENG, Y. Signcryption and its applications in efficient public key solutions. *International Workshop on Information Security* (1997), 291–312.

[103] ZHOU, J., DONG, X., CAO, Z., AND VASILAKOS, A. V. Secure and privacy preserving protocol for cloud-based vehicular dtns. *IEEE Transactions on Information Forensics and Security 10*, 6 (2015), 1299–1314.

[104] ZHOU, X., GANDHI, S., SURI, S., AND ZHENG, H. ebay in the sky: strategy-proof wireless spectrum auctions. *ACM MobiCom* (2008), 2–13.