Privacy-Preserving Multi-Quality Charging in V2G network

by

Miao He

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Applied Science
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2014

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

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

Abstract

Vehicle-to-grid (V2G) network, which provides electricity charging service to the electric vehicles (EVs), is an essential part of the smart grid (SG). It can not only effectively reduce the greenhouse gas emission but also significantly enhance the efficiency of the power grid. Due to the limitation of the local electricity resource, the quality of charging service can be hardly guaranteed for every EV in V2G network. To this end, the multi-quality charging is introduced to provide quality-guaranteed service (QGS) to the qualified EVs and best effort service (BES) to the other EVs. To perform the multi-quality charging, the evaluation on the EV's attributes is necessary to determine which level of charging service can be offered to the EV. However, the EV owner's privacy such as real identity, lifestyle, location, and sensitive information in the attributes may be violated during the evaluation and authentication. In this thesis, a privacy-preserving multi-quality charging (PMQC) scheme for V2G network is proposed to evaluate the EV's attributes, authenticate its service eligibility and generate its bill without revealing the EV's private information. Specifically, by adopting ciphertext-policy attribute based encryption (CP-ABE), the EV can be evaluated to have proper charging service without disclosing its attribute privacy. By utilizing group signature, the EV's real identity is kept confidential during the authentication and the bill generation. By hiding the EV's real identity, the EV owner's lifestyle privacy and location privacy are also preserved. Security analysis demonstrates that P-MQC can achieve the EV's privacy preservation, fine-grained access control on the EVs for QGS, traceability of the EV's real identity and secure revocation on the EV's service eligibility. Performance evaluation result shows that PMQC can achieve higher efficiency in authentication and verification compared with other schemes in terms of computation overhead. Based on PMQC, the EV's computation overhead and storage overhead can be further reduced in the extended privacy-preserving multi-quality charging (ePMQC) scheme.

Acknowledgements

First and foremost, I would like to express my deepest gratitude to my supervisor Professor Xuemin (Sherman) Shen for his continuous guidance and support on me to do this work during my study at the University of Waterloo. Without his guidance, this thesis would not have been possible. More importantly, Professor Shen is not only a good advisor, but also a shining example showing me how to face the challenges in both work and life.

I would also like to thank Professor Xiaodong Lin and Professor Kankar Bhattacharya as my thesis readers for contributing their precious time and effort in perfecting my work. I would like to thank Prof. Weihua Zhuang, Prof. En-hui Yang and Prof. Gordon Agnew, whom I have taken the courses from. They provide me with the necessary knowledge in order to do the research and complete the thesis.

I am also grateful to Mr. Kuan Zhang and other colleagues in the Broadband and Communication Research (BBCR) group for their warm friendships and helpful advices. It is my great honor to be a member of BBCR group at the University of Waterloo.

Finally, my deepest gratitude and love belong to my parents for their support and encouragement.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

At the beginning of the 21st century, US National Academy of Engineering had a debate to identify the most important single engineering achievement of the 20th century. While the revolutionary internet just ranking the thirteenth, the top one was the power grid, which was regarded as the most significant engineering achievement of the 20th century. The power grid is the largest interconnected machine on Earth. It consists of more than 9,200 electric generators and 300,000 miles of transmission lines. The total generating capacity of the power grid is more than 1,000,000 megawatts[4]. The power grid is linked with human's economy and society so tightly that everyone's life and work can be hardly independent of it. However, very few changes have taken place on the power grid system since its first scalable deployment in late 19th century. If Alexander Graham Bell and Thomas Edison were both transported to the 21st century, while Bell can hardly recognize the modern communication technology such as cell phone and voice over Internet Protocol (VoIP), Edison should be quite familiar with current power grid. Even though the power grid has been operated and maintained by dedicated professionals for decades, it is the truth that the power grid is becoming more and more heavily overburdened. According the statistic data from U.S. Department of Energy, the growth in peak demand for electricity has exceeded the transmission growth by almost 25% every year since 1982, due to the fast population growth and the rapid increasing number of household appliances[4]. Massive blackout occurs more and more frequently. Northeast blackout of 2003 affected 55 million

people[5]. 2005 Java-Bali blackout affected 100 million people in Indonesia[6]. 87 million people lost power for more than 48 hours in 2009 Brazil and Paraguay blackout[7]. Most recently, 670 million people's life and work were disturbed in July 2012 India blackout, which is the largest single blackout in human history[8]. The reliability of the power grid faces far more challenges than it has ever met before. Besides that, the mission for current power grid is no longer just simply keeping lights on. The future power grid should be also efficient, environmental friendly, secure and affordable.

1.1 Smart Grid

To address the major shortcomings of existing power grid, the next generation of power grid known as "smart grid" (SG) is introduced. The concept of SG first appears in the article "Toward a smart grid: power delivery for the 21st century" by Amin and Wollenberg[9]. According to the Independent Electricity System Operator's (IESO) definition, a smart grid is a modern electric system that uses communications, sensors, automation and computers to improve the flexibility, security, reliability, efficiency and safety of the electricity system. According to the comparison shown in Table 1.1, the SG includes several major characteristics shown below:

- Intelligent: SG can automatically sense system overload and reallocate the power resource to prevent or minimize the potential outrage, with much less responding time than that the manual operation requires.
- Efficient: In the current power grid, nearly 20% of the generation capacity is statically used to meet the peak demand, which stands for only 5% of the total time. In contrast, the power resource in SG can be dynamically allocated according to the fast varying consumer demands.
- Accommodable: Besides the centralized traditional bulk generation (coal, natural gas, hydro and nuclear), SG can integrate a large number of distributed and variable renewable energy sources such as solar, wind and tide.

Table 1.1: Comparison between the Smart Grid and the Existing Power Grid[1]

Existing Power Grid	**Smart Grid**
Electromechanical	Digital
One-way Communication	Two-way Communication
Centralized Generation	Distributed Generation
Hierarchical	Network
Few Sensors	Sensors Throughout
Blind	Self-monitoring
Manual Restoration	Self-healing
Failures and Blackouts	Adaptive and Islanding
Manual Check/Test	Remote Check/Test
Limited Control	Pervasive Control
Few Customer Choices	Many Customer Choices

- Resilient: SG should be protected by secure protocol to defend deliberate attack. Decentralized network structure should also be adopted to make the system more resistant to natural disaster such as hurricane and frozen rain.

- Environmental friendly: Renewable energy sources should stand for higher percentage in the total generation capacity of SG in order to reduce the greenhouse gas (GHG) emission.

Currently, there is no standard architecture for SG, due to the various communication protocols and power grid standards. The most widely accepted architecture for SG is the reference model (Figure 1.1) proposed by the U.S. National Institute of Standards and Technology (NIST). Seven important domains are defined as below:

- Bulk Generation domain: The Bulk Generation domain contains energy sources in bulk quantities. These energy sources can be either non-variable (coal and hydro) or variable (solar and wind).

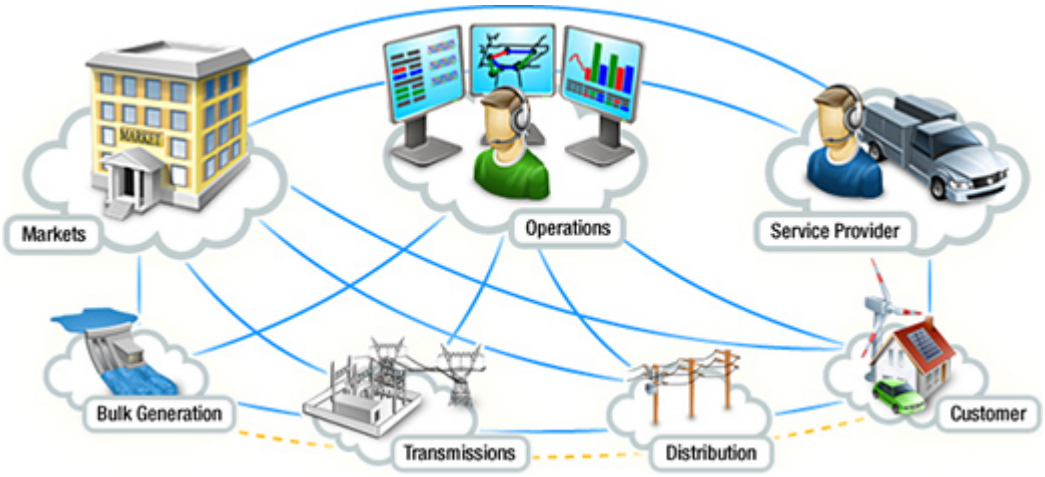

Figure 1.1: NIST Framework of Smart Grid[3]

- Transmission domain: Transmission domain is the backbone to massively transfer electricity over long distance. High voltage transmission lines, high voltage switches and high voltage transformers are key components in Transmission domain.

- Distribution domain: The Distribution domain includes the medium voltage transmission network (<50 kV) and distribution transformers (e.g. 12.47 kV to 120 V) to distribute the electricity to the end customers.

- Customer domain: The Customer domain consists of home, commercial/building and industrial users. The smart meter, which collects the customer's information about energy usage and patterns, is an essential device to control and manage the flow of electricity.

- Operations domain: The Operations domain is responsible for the management and control on the electricity flow in the SG, based on the information collected through the two-way communication network in the SG.

- Markets domain: The Markets domain operates and coordinates the electricity markets in the SG to build a competitive market environment.

- Service Provider domain: The Service Provider domain consists of third-party entities that provide new and innovative supporting services to meet the demand of markets.

1.2 Vehicle to Grid Network

With the growing global climate warming problem, GHG emission reduction has drawn significant attentions from government, industry and academia in recent years. Government of Canada has committed to reduce Canada's total GHG emission by 17% from 2005 to 2020[10]. Statistic data in Figure 1.2 shows that transportation accounts for 24% in Canada's total CO_2 emission, which is the largest single source of CO_2 emission[11]. Fuel switching is a strongly recommended solution to reduce the GHG emission from transportation[12]. Electrification of automobile transportation, especially deploying electric or hybrid automobiles, is regarded as an effective method to massively reduce the GHG emission.

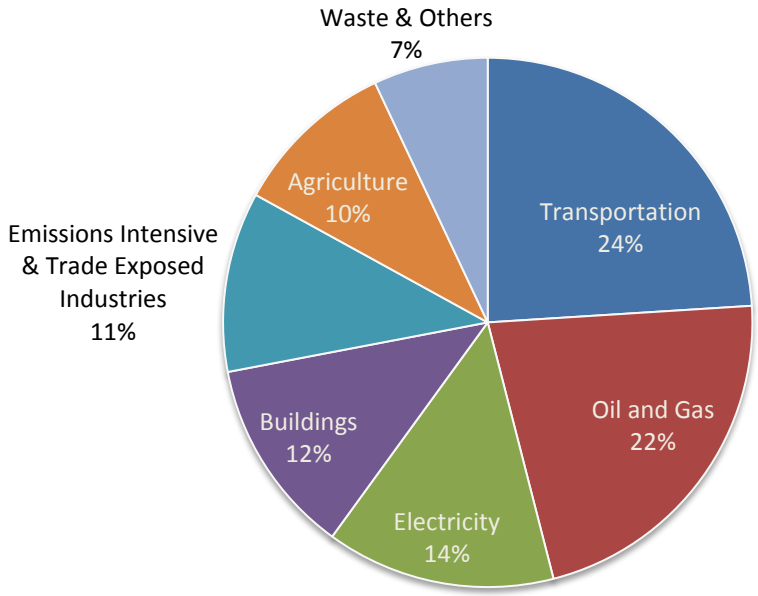

Figure 1.2: Source of GHG Emission in Canada 2010 by Economic Sector

To this end, large number of electric vehicles (EVs) should be deployed. Vehicle-to-grid (V2G) network is an infrastructure to support EVs, which uses the aggregated EVs as a distributed load or source to exchange power with the power grid[13]. Besides supporting EV and reducing GHG emission, V2G network can significantly enhance the efficiency of power grid by providing more flexible regulation service. Specifically, two kinds of regulation services can be provided from V2G network to the power grid. They are supply-demand equilibrium and frequency regulation[13] [14].

- Supply-demand equilibrium is to compensate for the peak load of the power grid with the power from the V2G network. There are two methods for the V2G network to get the power for supply-demand equilibrium. One is to reduce the charging power for the EVs under charging. The V2G network temperately reduces the power for the EV charging, and re-allocates the reduced power for supply-demand equilibrium. During this period, the charging power for the EVs will be temperately lower than their expected levels. Once the supply-demand equilibrium completes, the EVs regain their expected charging power. The other method is to make use of the energy stored in the EVs' batteries. Each EV can serve as a distributed source. Under V2G network's command, the EVs discharge their batteries to output the power for supply-demand equilibrium.

- Frequency regulation is to maintain the frequency of the power grid at a stable level by increasing or decreasing the generators' output power. Instead of directly adjusting the output power of the bulk generator, V2G network provides frequency regulation service to the power grid by commanding the EVs to charge or discharge at appropriate time. If the power grid has a demand on more power, more EVs in the V2G network discharge to provide the required power. Otherwise, more EVs under the V2G network's command to charge and consume more power in the power grid.

Compared with traditional methods to provide regulation service with bulk generators, V2G network can provide supply-demand equilibrium and frequency regulation with these benefits below:

1. High-utilization: The traditional method of supply-demand equilibrium to prevent outrage occurring is to install additional bulk generators, which generate additional electricity to meet the maximum peak demand. However, the maximum peak demand may only occur 80 - 100 hours each year[15]. Much of the generating capacity remains unused in most time of a year. In contrast, if the supply-demand equilibrium service is provided by V2G network, such low utilization can be prevented. In V2G network, the EVs can be regarded as a large number of distributed energy sources. By accumulating many EV batteries' discharging power, V2G network can provide considerable power to meet the peak demand of the power gird in a much more efficient way.

2. Fast-response: Typically, the duration of regulation service is several minutes, with a requirement on response time in no more than one minute[16]. To meet such requirement in a traditional way, the bulk generators need to operate at a minute by minute status, which not only faces a lot of technical difficulties but also causes addition mechanical wear and cost on bulk generators. On the other hand, V2G network can easily fulfill such requirement with little additional cost. The battery on the EV can respond in milliseconds, which is much faster than bulk generator can ever achieve. By controlling large number of EVs to transit between charging status and discharging status, V2G network can provide regulation service with a much faster response time.

3. Less additional investment: To the provide regulation service in a traditional way, additional facilities, such as spare bulk generators, transformers and transmission lines, need to be installed. Additional investment should also be done for bulk generator purchasing, installation and maintenance. In contrast, very little additional investment is required for V2G network to provide such regulation service, since the power for regulation service can be directly obtained from the EVs with existing V2G network infrastructure.

Due to the essentiality in both GHG emission reduction and efficiency enhancement in the power grid, V2G network is an important component of the SG. V2G network's major contribution on power grid efficiency promotion is to provide flexible regulation service

by utilizing the EV batteries. However, each individual EV battery with kilowatt-level power is too tiny to have an effective contribution to the demand of regulation service in power grid, which is normally megawatt-level at least. To this end, the aggregator (AGG) is introduced in V2G network to accumulate the large number of distributed EV batteries into a single load or source that can have a significant impact on the power grid[13] [17]. EVs have direct physical connection with the aggregator to exchange electricity. Consequently, V2G network includes these components as shown in Figure1.3.

- Aggregator: The Aggregator (AGG) accumulates the large number of distributed Electric Vehicle (EV) batteries into a single load or source as shown in Figure1.4. It is in the Distribution domain of the SG.
- Electric Vehicle: The Electric Vehicle (EV) is in the Customer domain of the SG to exchange power with the AGG.
- Independent System Operator: The Independent System Operator (ISO) is responsible for maintaining the stability of the power grid by monitoring and controlling the power flow in V2G network. It locates in the Operations domain of the SG.
- Energy Service Provider: The Energy Service Provider (ESP) is to provide electricity supply to charging AGGs. It also provides regulation service to the power grid with the power obtained from the discharging AGGs. Because of the ESP's essentiality in power distribution, it plays an important role in the Distribution domain of the SG.

1.3 Research Motivation and Objective

Due to the fast up-going oil price and the increasing environmental concerns, the EV, which has a steady up-going market penetration rate, can slowly but steadily take place of the traditional internal combustion engine vehicle and play a more and more important role in people's daily life. Different from traditional internal combustion engine vehicle, which is a pure mechanical device, the EV is the combination of vehicle technology, electricity

Figure 1.3: Structure of V2G Network

technology and information technology. While benefitting from the merits of information technology, the EV has to suffer corresponding privacy-preservation problems in communication network. In addition, because of the combination with vehicle technology and electricity technology, the privacy-preservation issues for the EV faces more challenges than that in traditional communication network. New privacy-preservation problems in terms of attribute privacy and lifestyle privacy are introduced in V2G network. Unique features are also addressed to the existing privacy-preservation problem such as location privacy, due to the combined characteristics of vehicle system and electricity system. Specifically, the challenges on privacy-preservation issues in V2G network can be classified into the following three aspects:

- **Attribute privacy:** Each individual EV is quite different from each other in many aspects. For instance, a bus consumes more power than a car does. It takes more time for a bus to charge the battery. In addition, a bus is used for public service, which is essential in a city's daily operation. Thus, a bus should have higher priority

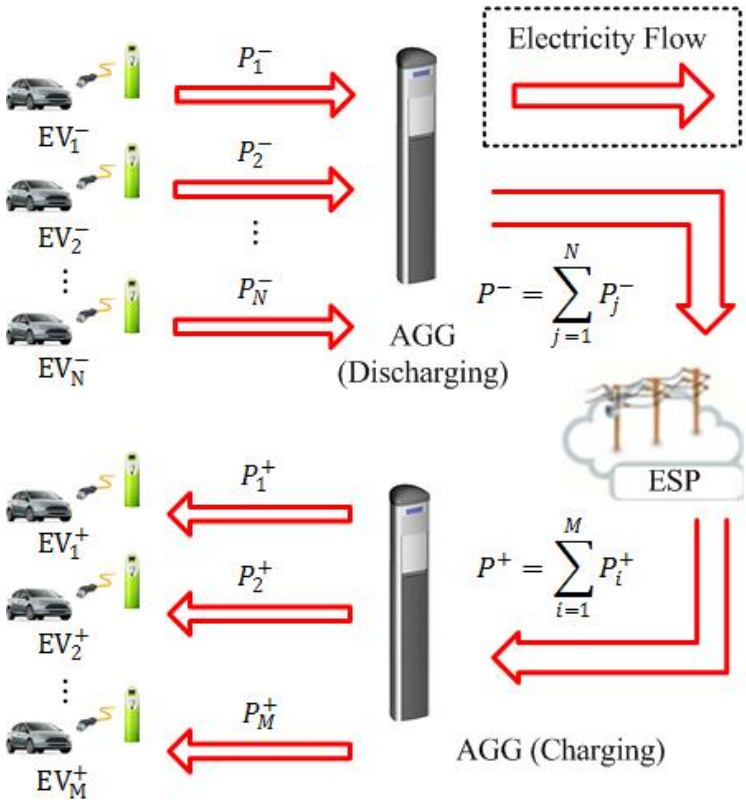

Figure 1.4: Aggregator in V2G Network

in charging services from the AGG. To the best of knowledge, different EVs may vary in preferred operation point (POP), battery volume, default ESP, charging priority, credit history, driving history, etc. These features can be regarded as the attributes on the EVs. It is reasonable for the AGG to provide charging services with different qualities to the EVs based on the evaluation on the EVs' attributes. However, some attributes such as POP, default ESP and credit history are quite sensitive. It is an open problem to preserve EV's attribute privacy when the EV is evaluated by AGG.

- **Lifestyle privacy:** While exchanging the electricity with the AGG, the EV's battery condition should be continuously monitored by AGG. There are two reasons for such continuous monitoring. First, improperly charging or discharging parameter

setting can be harmful to the EV's battery. The battery charging parameters need to be adjusted due to the varying EV battery status during the charging process. Thus, in order to prevent damages to the EV battery life, continuous monitoring on the EV battery condition should be performed to provide information for dynamic charging parameter adjustment[13]. Second, the total number of connecting EVs in V2G network is highly dynamic. Any EV may join or leave the V2G network at any time. In order to provide a relatively stable regulation service to the backbone power grid, continuous monitoring on the EV battery condition is necessary for the control on the EVs' arriving and departure. However, private information such as charging/discharging power, time, duration and state of charge is sensitive. By analyzing this monitoring information on a specified EV, such as when this EV started to charge or how much power this EV charged, the EV owner's lifestyle can be easily deduced.

- **Location privacy:** Mobility is a distinguishing feature of vehicle. Different from internal combustion engine vehicle, the EV only has very limited range, due to the low energy density of batteries compared to fossil fuel. In addition, the EV requires hours-long recharge time compared to the relatively seconds-fast process of refueling a tank. As a result, the EV needs to connect to the AGG to have its battery charged once it is possible, especially while parking at home or work place. Unfortunately, the EV owner's location privacy can be easily violated in such a scenario. The AGG and its belonging ESP can easily track the EV owner's location from such frequent connections.

In conclusion, the privacy-preservation concern becomes a significant issue in V2G network[18][19]. Without appropriate privacy-preserving mechanics, customers may be reluctant to join in the V2G network. As a result, the replacement of internal combusting engine vehicle, the modernization of the power grid and the reduction in GHG emission all may be hindered. Thus, it is paramountly necessary to solve the privacy-preservation problem in V2G network.

1.4 Problem Formation

In V2G network, the local total electricity power of each AGG is limited. If too many EVs request charging service from one particular AGG at the same time, the total required power may be more than the maximum supply power that the AGG can provide. In such scenario, all the EVs have to share the maximum supply power from the AGG. The simplest charging power allocation scheme is to equally allocate the charging power to each EV. However, such simple scheme makes all the EVs' charging power below their preferred operation points (POPs), which means none of the EVs can have quality guaranteed charging service. Each EV can not receive its expected charging power from the AGG. It contradicts some important EVs' requirements on charging service quality and ignores the market's demands on diverse charging service qualities[20][21]. For instance, some EVs such as police vehicles, ambulances and taxis are used for public service. Their charging power should be guaranteed to reduce their charging time as much as possible due to their essentiality in a city's public service. Some private EVs may be also willing to pay more money to the electricity service provider (ESP) for priority charging service. Considering this, a novel charging scheme with multi-quality services i.e., "quality guaranteed service" (QGS) and "best of effort service" (BES), as shown in Figure 1.5 is introduced. In QGS, the charging power for the EV can be guaranteed at its POP. In BES, the EV's charging power varies depending on the remaining power after QGS in the AGG.

To determine each EV's service quality, the AGG should evaluate individual EV's attributes, such as public/private use, priority service contract, POP level, credit history level, driving history level, default ESP etc. The evaluation is based on a policy made by AGG, according to its local electricity resource condition. The different AGGs' policies may also be different due to their different local resource conditions and different default ESPs. For example, "private vehicle" AND "priority service contract" OR "public vehicle" OR "Ambulance" can have QGS in a resource abundant AGG. In a resource limited AGG, the policy may be 'public vehicle" AND "Ambulance", which means neither any private vehicles nor any public vehicles except the ambulances can have QGS.

However, the privacy concern is an obvious barrier to the proposed multi-quality charging scheme in V2G network.

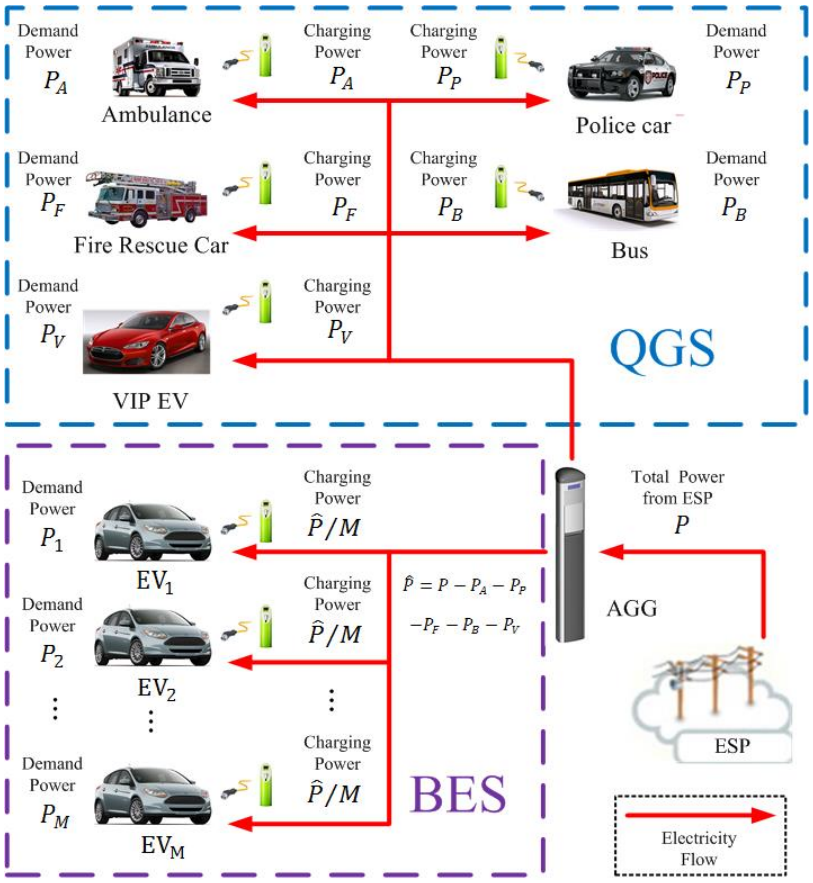

Figure 1.5: QGS and BES in V2G Network

- The AGG's evaluation on the EV is necessary to determine its service quality. The EV's attributes, such as service contract, credit history, driving violation history, default ESP etc, is sensitive information. If this kind of information is directly revealed to the AGG, the EV owner's privacy could be violated. For instance, the EV owner's occupation can be obtained by analyzing the charging plan in the service contract. The EV owner's financial situation can also be inferred from inspecting the credit history.

- Performing continuous monitoring on the EV battery's state of charge is essential during the charging service. However, such continuous monitoring reveals the detail

of the EV battery status to the AGG. By analyzing this information, the EV owner's lifestyle and occupation may be deduced. For example, unusual charging with a small amount of electricity indicates the EV may be not frequently used. The owner of the EV may be a retired man who usually stays at home. Frequent charging with a lot electricity implies the owner of the EV may be a salesman who always goes on business. Target marketing can be performed based on this information. Unexpected advertising such as fliers, emails and phone calls may arrive to the EV owners.

- The location of each charging port is known to the AGG. Once the EV parks in a lot and plugs into the charging port, the AGG can obtain that EV's very exact position. If the AGG can also get the EV's real identity, the EV owner's location can be exposed to the AGG.

Motivated by the privacy concerns above, the goal of this thesis is to design a privacy-preserving multi-quality charging (PMQC) scheme in V2G network. While providing multi-quality charging services to the EVs , the proposed scheme should solve the privacy-preservation problems listed above. To this end, by exploiting the unique features of V2G network, a novel evaluation and authentication protocol based on proper encryption and signature algorithms is proposed to achieve the privacy-preservation in the multi-quality charging scheme. Specifically, the contributions can be summarized in three-fold:

1. An evaluation mechanism on the EV's attributes is proposed to determine the EV's charging service quality. While achieving fine-grained access control on the qualified EV for QGS, the EV's attributes are kept secret to the AGG during the evaluation.

2. The EV's real identity is kept confidential to the AGG when the AGG performs the authentication and bill generation on the EV. Based on this, the EV owner's lifestyle privacy and location privacy are also preserved.

3. Performance evaluation shows the computation overhead of authentication in the proposed scheme can achieve higher efficiency, compared with other authentication schemes in V2G network.

1.5 Literature Review on Related Work

Currently, the research on privacy-preservation in the V2G network is still at the early stage. The researches focus on various issues including security architecture, authentication mechanism and key management in V2G network.

Yang *et.al* [22] propose a privacy-preserving rewarded architecture, which focuses on the anonymous authentication. The main idea is to hide the EV's real identity by adopting the ID-based restrictive partially blind signature [23], when the EV is authenticated by the AGG. The EV can get the charging service from the AGG if and only if the EV provides a valid permit, which is secretly issued by the control center. Even though the AGG can obtain all the detail information about the EV during the charging service, it can hardly link this detail monitoring information with any specified EV owner's real identity. In this way, the EV owner's location privacy and lifestyle privacy are both preserved. Besides the anonymous authentication, a rewarded architecture is also introduced to encourage the EVs to participate in the V2G network.

Tseng further develops Yang's work. In [24], the certificate-less public key cryptography is introduced to simplify the certificate management and overcome the key escrow problem in Yang's scheme.

Liu *et.al* propose an authentication scheme in V2G network. In [25], Liu *et.al* claim that the EV should be associated with a default interest group. Besides charging from the default group, the EV may also visit other groups and have charging service from them due to the EV's mobility. In such scenario, two charging service modes are defined for the EV, home mode and visiting mode. Specifically, home mode is for the EV having charging service from the default AGG. Visiting mode is for the EV having charging service from the other interest group's AGG. An aggregated authentication scheme is proposed to authenticate the EV in either home mode or visiting mode, without revealing its real identity to the AGG. The anonymous authentication is based on the aggregated proof, which is developed from the coexistence-proof in radio frequency identification (RFID). In addition, the authentication can also be performed for multiple EVs at the same time. Thus, the computational overhead for authentication is significantly reduced. Meanwhile, the battery status monitoring data can also be periodically collected by AGG without

compromising individual EV's privacy.

In [26], Tseng proposes a robust aggregated message authentication protocol for privacy-preservation in the V2G network. The computation overhead is significantly reduced by utilizing authentication aggregation and batch verification techniques.

In [27], Liu *et.al* investigate a new security problem based on the EV's varying battery status. While interacting with the AGG, the EV's battery may be in one of the following states: charging, fully-charged (FC) and discharging. The EV's private information such as location, occupation and lifestyle may be obtained by AGG, through analyzing the battery status information under different battery states. To this end, a battery status-aware authentication scheme is proposed to prevent the EV owner's privacy from being violated. Specifically, three security measures are performed during the three different battery status transitions. First, during the charging-to-FC state transition, an aggregated-identifier is proposed to ensure that each EV can be authenticated without revealing its real identity. Second, during the transition of FC-to-discharging, anonymous data transmission is achieved by selective disclosure based challenge-response authentication. Third, during the discharging-to-charging transition, an aggregated status reporting is performed in order keep each EV batteries' power level confidential to the AGG.

Besides the privacy-preservation issues, there are some works on other security issues in V2G network. Guo *et.al* [28] propose a batch authentication protocol for fast authentication in V2G network. The motivation comes from the fact that the EV can only have very limited connection time for data transmission during driving. In this scheme, the AGG aggregates the received signatures from multiple EVs into a batch at intervals. Then the AGG verifies the batch of EVs' signatures, instead of verifying each EV's signature. Vaidya *et.al* [29] propose a multi-domain network architecture for the V2G network. They claim that the utilities in the V2G network may be belonged to different independent realms. The authentication and verification should be performed across different realms. In such scenario, challenges arise in the key management among different realms. To this end, a multi-domain network architecture with a hybrid PKI model is introduced to solve such security challenge.

There are more works focusing on the security issues in the SG. Liang *et.al* [30] propose a

usage-based dynamic pricing scheme for the SG in a community environment, which enables the electricity price to correspond to the electricity usage in real time. While supporting real-time dynamic pricing in an efficient and privacy-preserving manner, the privacy of the customer is protected by restricting the disclosure of the individual electricity usage to the community gateways. Wen *et.al* [31] propose a novel privacy-preserving range query scheme over encrypted metering data to address the privacy issues in financial auditing for SG. The proposed scheme allows a residential user to store metering data on a cloud sever in an encrypted form. When financial auditing is needed, an authorized requester can send its range query tokens to the cloud sever to retrieve the metering data. While the data confidentiality and query privacy are preserved, only the authorized requesters can obtain the query results. Li *et.al* [32] propose an efficient authentication scheme that employs the Merkle hash tree technique to secure SG communication. Detail security analysis indicates that the proposed scheme can be resilient to the replay attack and the message modification attack.

However, all the works above simply assume all the EVs are identical and ignore the difference in attributes among the EVs. In addition, none of them consider the market's demand on diverse EV charging service qualities and the corresponding privacy-preservation problem. In this thesis, a privacy-preserving multi-quality charging (PMQC) scheme in V2G network is proposed to evaluate and authenticate the EV without violating its private information. Specifically, an evaluation mechanism is introduced to determine the EV's charging service quality according to the EV's attributes. Based on the ciphertext-policy attribute based encryption (CP-ABE), the PMQC prevents the EV's attributes from being disclosed to the AGG during the evaluation. Furthermore, an authentication protocol based on group signature is constructed in the PMQC to verify the EV's eligibility for charging service without obtaining its real identity.

1.6 Thesis Outline

The remainder of the thesis is organized as follows:
Chapter 2 introduces the related encryption and signature algorithms. The system model

is defined in Chapter 3, including network model, trust model and security requirements. Chapter 4 formulates the proposed privacy-preserving multi-quality charging (PMQC) scheme in V2G network. Chapter 5 presents the security analysis and performance evaluation on the PMQC. Based on the PMQC in Chapter 4, the extended privacy-preserving multi-quality charging (ePMQC) scheme in V2G network and corresponding performance enhancement are introduced in Chapter 6. Chapter 7 closes the thesis with conclusions and the future work.

Chapter 2

Cryptography Fundamental

This chapter introduces the related cryptography fundamental. The properties of bilinear map is briefly described in Section 2.1. Then the attribute based encryption and the group signature are separately introduced in Section 2.2 and Section 2.3.

2.1 Bilinear Map

Bilinear map is an important algebra structure in cryptography. The exact mathematic definition of bilinear map is very complex and abstract. Because this thesis focuses on the privacy-preservation issues in V2G network, only the properties of bilinear map are introduced in this section to help the readers have a better understanding of following part of the thesis.

$\mathbb{G}$ and $\mathbb{G}_T$ are assumed to be two multiplicative cyclic groups of prime order p. The map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is said to be a bilinear map, if the group operation in $\mathbb{G}$ and the map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ are both efficiently computable.

The bilinear map e has the following properties:

1. **Bilinearity:** For any $u, v \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p^*$, we have $e(u^a, v^b) = e(u, v)^{ab}$. Specifically, $e(u_1 \cdot u_2, v) = e(u_1, v) \cdot e(u_2, v)$.

2. **Non-degeneracy:** $e(g, g) \neq 1$, where g is a generator of $\mathbb{G}$.

3. **Computability:** There is an efficient algorithm to compute $e(u, v)$ for $\forall u, v \in \mathbb{G}$

Here $\mathbb{Z}_p^*$ denotes the multiplicative integer group under multiplication modulo p, satisfying $\mathbb{Z}_p^* = \{z \in \mathbb{Z}_p \mid \gcd(z, p) = 1\}$, where $\mathbb{Z}_p$ is the set of integers $\{0, 1, 2, \cdots, p-1\}$. $\gcd(z, p)$ is the function to get the greatest common divisor of integer z and p.

2.2 Attribute-Based Encryption

Asymmetric cryptography is a fundamental security ingredient in cryptosystems, applications and protocols. The concept of asymmetric cryptography was first introduced by W. Diffie and M. Hellman[33] in 1976. Different from that in the symmetric cryptography, the sender Bob and the receiver Alice in the asymmetric cryptography do not need to securely share a key in advance. Instead, the receiver Alice generates a pair of private and public keys. The public key, which is published to the public by Alice, is used by the sender Bob to encrypt the plaintext. The private key, which is kept confidential by Alice, is used by Alice to decrypt the ciphertext from Bob. Typical asymmetric encryption algorithms such as RSA and ElGamal are designed to securely share the secret information with a known specific user. What these algorithms have in common is to require the sender to determine the target receiver before encryption. Then the sender encrypts the secret information with the target receiver's public key. For example, the sender Bob first needs to determine it is Alice who is the target receiver. Then he encrypts the message with Alice's public key and sends the ciphertext to her. However, those algorithms with such requirement may not be suitable for the scenario like cloud computing, where the sender wishes to share the data to the receivers according to some policies on the receiver's credentials.

To solve that problem, Sahai and Waters [34] introduce the concept of attribute-based encryption (ABE). In ABE, the plaintext is not encrypted with one specific receiver's public key. Instead, the plaintext is encrypted with a predicate f() defined by the sender. In this predicate f(), the sender can express how he wants to securely share this plaintext. The receiver has the private keys associated with his credentials S. If and only if $\mathrm{f}(S) = 1$ can

the receiver decrypt the ciphertext under the predicate f(). In Sahai and Waters work, the receiver's credentials called "attributes" is a set of string, and the predicate called "policy" is described by a formula over these attributes.

Based on the initial work of Sahai and Waters, the concept of attribute-based encryption is further developed. Two forms of ABE are addressed, Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE.

2.2.1 Key-Policy Attribute-Based Encryption

In Key-Policy ABE (KP-ABE), the ciphertext is encrypted with a set of attributes. The receiver's private key is associated with a policy based on these attributes. The receiver is able to decrypt the ciphertext, if the ciphertext's attributes match the policy in the receiver's private key. For example, the Document A is KP-ABE encrypted with the following attributes: "Electrical and Computer Engineering", "Graduate Student", "Network Security". The Document B is KP-ABE encrypted with the following attributes: "Electrical and Computer Engineering", "Faculty", "Network Security". The Faculty A specializing in image processing is from Electrical and Computer Engineering. His private key is associated with the policy {"Electrical and Computer Engineering" AND "Faculty" AND "Image Processing"} OR "Graduate Student". The Document A's attributes match the Faculty A's policy. Thus, the Faculty A can decrypt the ciphertext and get the Document A. In contrast, the Document B's attributes mismatch the Faculty A's policy. Faculty A cannot decrypt the corresponding ciphertext to view the Document B.

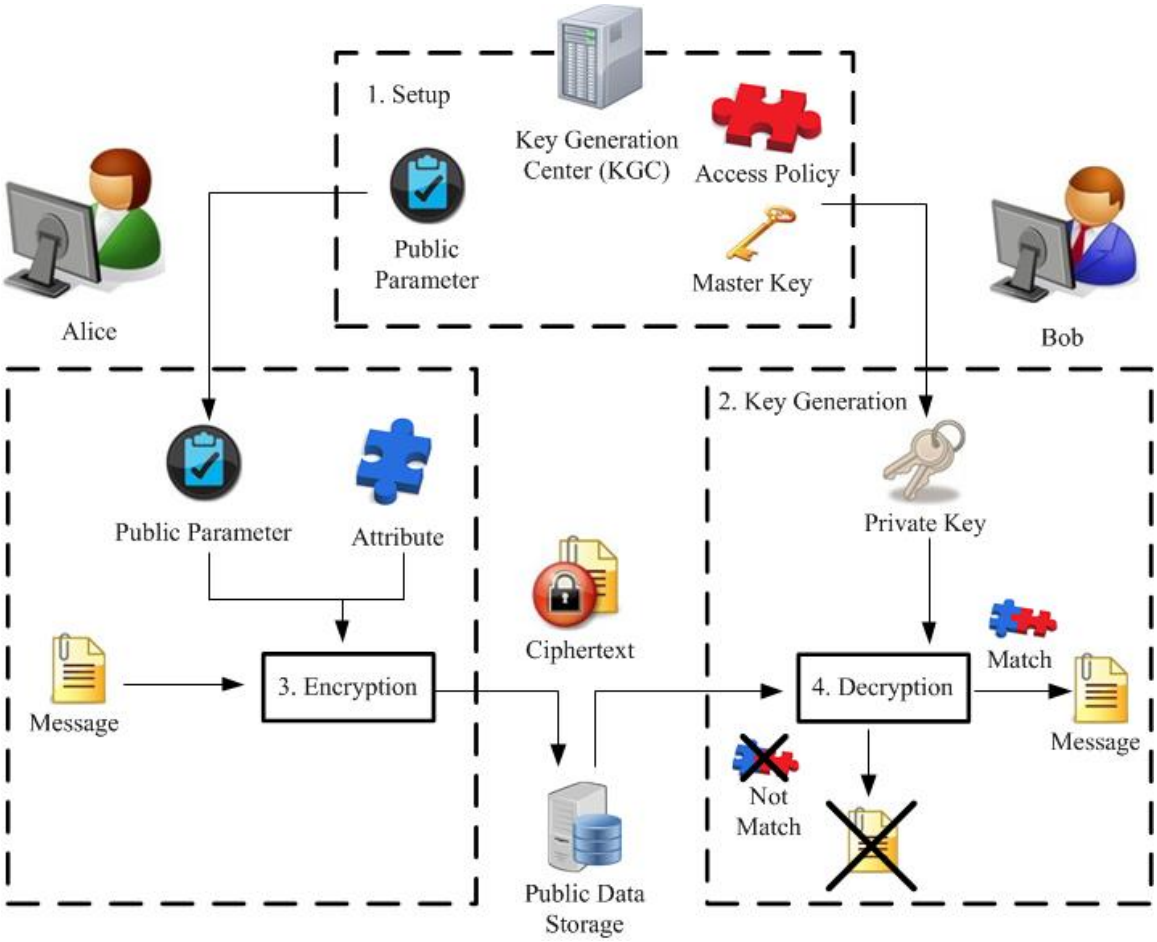

Figure 2.1: Key-Policy Attribute Based Encryption System

Goyal *et.al* [35] first introduce the concept of KP-ABE. In his work, a general KP-ABE scheme with better applicability than that in [34] is proposed. In Goyal's construction, the ciphertext is encrypted with a set of attributes and the receiver's private key is associated with a policy which can be described with a tree structure. The tree structure is a fine-grained access control structure supporting "AND", "OR" and "$Threshold$" operations. The scheme is proved to be Chosen Ciphertext Attack (CCA) secure under the decisional-Bilinear Diffie-Hellman (d-BDH) assumption in the standard model. There are four phases in Goyal's proposed KP-ABE scheme as shown in Figure 2.1:

- **Setup:** The input is a security parameter ψ. The outputs are the public parameter PK and the master key MK. The Setup phase is performed by Key Generation Center (KGC), which is a fully trusted entity.

- **Key Generation** $(PK, MK, \mathbb{A})$**:** The inputs of the Key Generation phase are the public parameter PK, the master key MK and the policy which is expressed in the access structure $\mathbb{A}$. The output is the private key SK associated with access structure $\mathbb{A}$. This phase is performed by the KGC. The private key SK should be delivered to the corresponding receiver through secure channel.

- **Encryption** (PK, M, S)**:** The inputs are the public parameter PK, the plaintext M and the attribute set S. The output is the ciphertext CT associated with the attribute set S.

- **Decryption** (PK, SK, CT, S)**:** The inputs are the public parameter PK, the receiver's private key SK and the ciphertext CT with the attribute set S. The receiver performs this phase to decrypt CT. If the ciphertext's attribute set S matches the policy that associated with the receiver's private key, the Decryption phase can be performed successfully to output the plaintext M.

Ostrovsky *et.al* [36] further develop Goyal's work. While maintaining the CCA security under the d-BDH assumption in the standard model, Ostrovsky's scheme adds "NEG" operation to describe the access control structure. With "AND", "OR", "$Threshold$" and the newly added "NEG" operation, the access control structure becomes more flexible.

2.2.2 Ciphertext-Policy Attribute-Based Encryption

Different from that in the KP-ABE, the ciphertext in the Ciphertext-Policy ABE (CP-ABE) is encrypted with a policy by the sender, and the receiver's private key is associated with the attributes. The receiver can decrypt the CP-ABE ciphertext if and only if a matching between the ciphertext's policy and the private key's attributes exists. The structure of a CP-ABE system is shown in Figure 2.2.

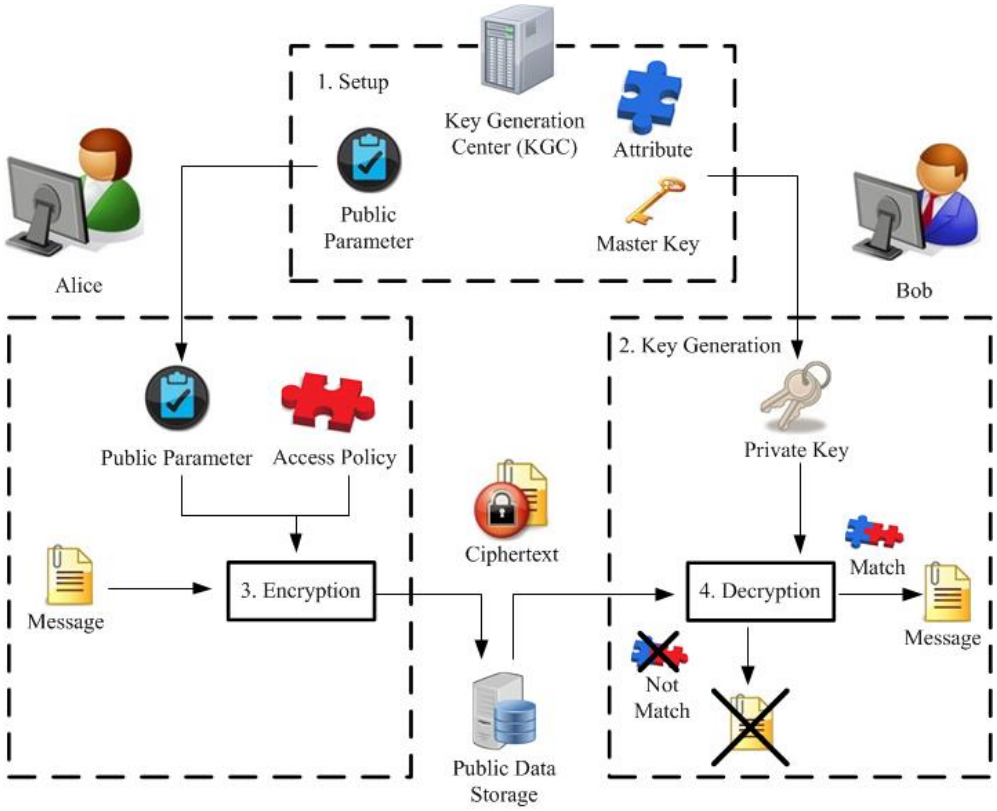

Figure 2.2: Ciphertext-Policy Attribute Based Encryption System

Bethencourt *et.al* [37] first explicitly propose a CP-ABE scheme. Similar to the scheme in [35], the policy is described with a tree structure, which is also a fine grained access control structure supporting "AND", "OR" and "$Threshold$" operations. Besides that, Bethencourt's scheme supports private key delegation. Thus there are five phases in the scheme:

- **Setup:** This phase takes a security parameter ψ as input and outputs the public parameter PK and the master key MK.
- **Key Generation** (MK, S)**:** The Key Generation phase in the CP-ABE takes the master key MK and the receiver's attribute set S as input. The output is the private

key SK with the receiver's attribute set S. The output is the receiver's private key SK, which should be delivered to the receiver through secure channel.

- **Encryption** $(PK, M, \mathbb{A})$**:** The inputs are the public parameter PK, the plaintext M and the access structure $\mathbb{A}$ defined by the sender. The outputs are the access structure $\mathbb{A}$ and the ciphertext CT, which is encrypted under the access structure $\mathbb{A}$.

- **Decryption** $(PK, SK, CT, \mathbb{A})$**:** The inputs are the public parameter PK, the receiver's private key SK and the ciphertext CT with corresponding access structure $\mathbb{A}$. If the attribute set S of the receiver's private key matches the access structure $\mathbb{A}$ associated with ciphertext CT, the ciphertext CT can be decrypted.

- **Delegation** (SK, S')**:** This phase updates the attributes of the private key. It takes the new attribute set S' and the old private key SK with attribute set S as input. The output is the new private key SK' with the new attribute set S'.

Bethencourt's scheme achieves analogous expressiveness and fine-grained access control. The scheme is proved to be CCA secure under the Generic Bilinear Group [38] in the random oracle model. But the security proof is less than ideal, because the Generic Bilinear Group assumption is too strong, which assumes the attacker needs to access an oracle in order to perform any group operation [2].

To achieve a better security, Cheung *et.al* [39] propose a scheme which is proved to be CCA secure under the d-BDH assumption in the standard model. However, this scheme only supports "AND" and "NEG" operations in the access structure.

To overcome the shortcoming of Cheung's scheme, Goyal *et.al* [40] propose a new CP-ABE scheme with a bounded size access tree. Two parameters are set to limit the height and the number of children in the access tree. In addition, an "universal access tree" is also introduced to construct a mapping in order to transform a KP-ABE system into a CP-ABE system. The scheme is proved to be CCA secure under the d-BDH assumption in the standard model.

Waters *et.al* [2] further develop the CP-ABE. The efficiency in Water's scheme is significantly improved by expressing the access control structure with a Linear Secret Sharing

Table 2.1: Comparison of the CP-ABE Schemes[2]

Scheme	Ciphertext Size	Private Key Size	Enc. Time	Assumption
Bethencourt's	$\mathcal{O}(n)$	$\mathcal{O}(\mathbb{A})$	$\mathcal{O}(n)$	Generic Group
Goyal's	$\mathcal{O}(U \cdot n_{max}^{3.42})$	$\mathcal{O}(n_{max}^{3.42} \cdot \mathbb{A})$	$\mathcal{O}(n_{max}^{3.42} \cdot U)$	d-BDH
Waters's First	$\mathcal{O}(n)$	$\mathcal{O}(\mathbb{A})$	$\mathcal{O}(n)$	d-Parallel BDHE
Waters's Second	$\mathcal{O}(n)$	$\mathcal{O}(k_{max} \cdot \mathbb{A})$	$\mathcal{O}(n)$	d-BDHE
Waters's Third	$\mathcal{O}(n^2)$	$\mathcal{O}(k_{max} \cdot \mathbb{A} + n_{max})$	$\mathcal{O}(n^2)$	d-BDH

Scheme (LSSS) matrix. Three constructions are provided under three different security assumptions. The first construction is the simplest one with the highest efficiency. It is proved to be CCA secure under the decisional-Parallel Bilinear-Diffie Hellman Exponent (d-Parallel BDHE) assumption, which is a relatively strong secure assumption in the standard model. The second construction is CCA secure under the slightly weaker decisional-Bilinear-Diffie Hellman Exponent (d-BDHE) assumption in the standard model with a little efficiency drop. The third construction provides the strongest security. It is proved to be CCA secure under the weak d-BDH assumption in the standard model. Even though its strong security is achieved at the expense of efficiency deterioration, it still has a better efficiency than that in Goyal's scheme [40]. The comparison of efficiency among the CP-ABE schemes is shown in Table 2.1. Here n is the size of an access formula, $\mathbb{A}$ is the number of attributes in a user's private key, T is the number of nodes satisfied of a formula by a user's attributes, and U is the number of attributes defined in the system.

2.2.3 Comparison of the Encryption Algorithms

The Table 2.2 is a comparison of some typical asymmetric encryption methods. Here "Para" indicates the public parameter in the specified system. "ID" indicates the identity of the Decipherer in IBE. "S" indicates the attributes in ABE. "A" is the access control structure based on the attributes S. From the comparison we can clearly see that both

KP-ABE and CP-ABE are much more flexible in secure mechanism design. Thus, the first CP-ABE construction of Waters's work [2] is adopted in the thesis.

2.3 Group Signature

The digital signature is another important application of asymmetric cryptography. The concept of digital signature is first described by W. Diffie and M. Hellman [33]. The digital signature on a message is generated by the signature signer with his private key. Then the message with corresponding digital signature is transmitted to the receiver. By verifying the digital signature with the signature signer's public key, the receiver can perform authentication on the signature signer, check the integrity and ensure the non-repudiation of the message.

In the typical digital signatures such as RSA and DSA, the signature signer's identity needs to be revealed to the public. This feature makes the typical digital signatures hardly satisfy the requirement of anonymity in some scenarios such as electronic voting and bid inviting, where the identity of the signer should be kept secret. To this end, the concept of group signature is introduced by Chaum *et.al* [41] in 1991. In group signature, the singer should be a member of a certain group. As a member of a group, the signer can anonymously sign a message on behalf of its belonging group. While verifying the group signature to check the message's integrity and ensure its non-repudiation, the receiver can only perform the authentication on the group instead of the individual who signs the group signature. In this way, the signer's identity is kept confidential to the receiver. In addition, there should be a group manager in each group, who is responsible for group member managing and tracking the identity of the signer in the event of disputes. Generally, there are following characteristics of the group signature [42][43]:

- **Anonymity:** Given a valid group signature, it is computationally impossible for any entity except the group manager to reveal the identity of actual signer.

Table 2.2: Comparison of the Asymmetric Encryption Algorithms

	Traditional Asymmetric Encryption	Identity Based Encryption	KP-ABE	CP-ABE
Master Key MK	None	Randomly selected by KGC	Randomly selected by KGC	Randomly selected by KGC
Private Key SK	Randomly selected by Decipherer	$SK = (Par, ID, MK)$ generated by KGC	$SK = (Par, A, MK)$ generated by KGC	$SK = (Par, S, MK)$ generated by KGC
Public Key PK	$PK = (Par, SK)$ generated by Decipherer	$PK = (Par, ID)$ generated by Encipherer	$PK = (Par, S)$ generated by Encipherer	$PK = (Par, A)$ generated by Encipherer
Public Key Certificate	Required	Not required	Not required	Not required
Relation between PK and SK	1. One SK can only map to one PK 2. Only one PK can be chosen by Encipherer 3. No restriction on Decipherer's decryption capability	1. One SK can only map to one PK 2. Multiple PKs can be chosen by Encipherer 3. The Decipherer's decryption capability is restricted by KGC	1. Multiple SKs can map to multiple PKs 2. Multiple PKs can be chosen by Encipherer 3. The Decipherer's decryption capability is restricted by KGC and Encipherer	1. Multiple SKs can map to multiple PKs 2. Multiple PKs can be chosen by Encipherer. 3. The Decipherer's decryption capability is restricted by KGC and Encipherer

- **Traceability:** The group manager has the full capacity to open a valid group signature from his group and trace the identity of the individual who actually signs the group signature.
- **Unforgeability:** Only the valid group member can generate the group signature on behalf of its belonging group.
- **Exculpability:** Neither a group member nor the group manager can sign a group signature on behalf of other members.
- **Unlinkability:** It is computationally impossible to judge whether or not two valid group signatures are generated by the same individual.
- **Conspiracy Attack Resistance:** It is impossible for a subset of group members to conspire to generate a special group signature, which is valid but impossible for the group manager to open.

Chen *et.al* [44] provide solutions to the some open issues mentioned in the Chaum's work. First of all, dynamic group member participation is allowed in the proposed scheme. In addition, some new concepts, such as "total convertible group signature", "selective convertible group signature" and "threshold group signature", are introduced to the group signature.

However, the length of the public key and the length of the group signature are linear with the number of group members in both Chaum's and Chen's schemes. It seriously constrains the application of group signature in large systems, since the efficiency dramatically deteriorates with the increase of the group size. To overcome such challenge, Camenisch *et.al* [45] propose an efficient group signature scheme by introducing the concept of signature of knowledge. First of all, the length of the group public key and the length of the group private key are independent of the number of group members, which means that they are fixed in length. In addition, the scheme allows the group manager to add new group members without updating the group public key. Benefiting from these two features, the efficiency is significantly improved in Camenisch's scheme. While further improving the

efficiency, Ateniese *et.al* [42] propose a conspiracy attack resistant group signature scheme based on Camenisch's work.

All the group signature schemes above do not consider the group member revocation problem, which is necessary in the the group management. Bresson *et.al* [46] first propose a scheme including group member revocation. But the computation overhead of group signature verification in Bresson's scheme is linear with the number of revoked members. Based on Bresson's work, Camenisch *et.al* [47] improve the revocation efficiency by adopting a dynamic accumulator. Boneh *et.al* [48] introduce a new revocation mechanism named Verifier-Local Revocation (VLR). In Boneh's scheme, only the signature verifiers are notified about the revocation list, which includes a fragment of the revoked users' private key. As a result, the revocation process is simplified. Based on the previous work, Boneh *et.al* [49] further develop the VLR revocation mechanism. Besides the considerable efficiency promotion in revocation, the size of the group signature is also significantly reduced to approximately the same size of a standard RSA signature.

In recent years, more schemes on group signature in the standard model are proposed [50][51][52]. However, the strong security of these schemes comes at the expense of high complexity and low efficiency. Considering this, Boneh's scheme [49] is adopted in the thesis.

Chapter 3

System Model and Security Requirements

In this chapter, the system model of the proposed privacy-preserving multi-quality charging (PMQC) scheme is introduced in Section 3.1. Then the security requirements on PMQC are defined in Section 3.2.

3.1 System Model

The electricity flow in V2G network can be unidirectional or bidirectional. In the bidirectional V2G network, the AGG can provide the power grid with regulation service, by letting connected EVs charge to consume power from the power grid or discharge to feed power back to the power grid. However, the implementation of bidirectional electricity flow in V2G network has to face the various challenges in terms of technique, capital and market. For example, the anti-islanding protection and other interconnection issues are addressed in the bidirectional power grid[53]. To support the bidirectional electricity flow, considerable investments in the electricity infrastructure updating on the current unidirectional power grid are required. It is also speculated that consumers may be resistant to allowing the utility company to pull energy from their batteries[54]. As a result, the unidirectional

V2G network is more practical in implementation based on current well-developed unidirectional electricity infrastructures[53]. In the unidirectional V2G network, the EVs can only charge power from the AGG. By varying the EVs' charging power around the EVs' preferred operation points (POP), the unidirectional V2G network can also provide regulation service to the power grid[55]. Thus, the electricity flow in V2G network is assumed to be unidirectional in the system model. The "unidirectional V2G network" in the following part of the thesis is referred as the "V2G network".

To have charging service from the AGG, the EV should be authenticated by the AGG, which checks the EV's eligibility for the charging service. In addition, the AAG or the EV should have a default Electricity Service Provider (ESP). If the EV and its visiting AGG are in the same ESP, the AGG's authentication on the EV can be easily performed. However, problems arise in the authentication, if there are multiple different ESPs in a region as shown in Figure 3.1. Due to the EV's mobility, it is reasonable that the EV may move to the area covered by a non-default ESP and visit the AGG of that non-default ESP. For example, there are three ESPs in the Cambridge- Kitchener- Waterloo area, Waterloo North Hydro Inc., Kitchener Wilmot Inc., and Cambridge and North Dumfries Hydro Inc.. Alice may live in Waterloo with the default ESP Waterloo North Hydro Inc.. Her office may be in Cambridge, where the electricity is provided by Cambridge and North Dumfries Hydro Inc.. During the work time, Alice often goes to Kitchener to do business. In such scenario, it is a problem to perform the authentication on Alice's EV across different ESPs. The major obstacle is the fact that the different ESPs are market competitors, which makes the different ESPs be unwilling to share their customers' information with each other. To this end, the Electric Vehicle Administration (EVA), which is an independent non-profit institution, is introduced in the system model in this thesis to manage all the EVs in the V2G network, and build a unified authentication mechanism on the EVs among different ESPs. Specifically, the EVA issues a secret private key to each eligible EV when it registers itself to the EVA. With the private key, the EV can answer the AGG's challenge and pass the authentication, no matter the EV and the AGG are in the same ESP or not. Thus, authentication on the EVs across different ESPs can be achieved. Besides the private key issuing, the EVA is also responsible for the EVs' attributes allocation, private key revocation and electricity fees charging.

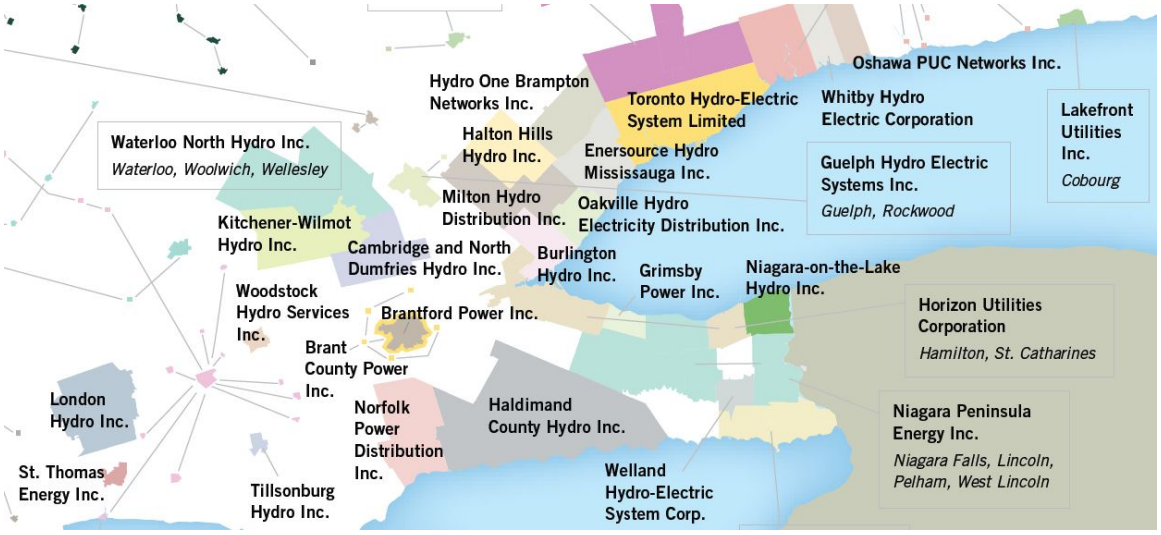

Figure 3.1: ESP Distribution in Southern Ontario

As a result, there are four entities in the system model as shown in Figure 3.2. They are Electric Vehicle Administration (EVA), Aggregator (AGG), Electric Vehicle (EV) and Electricity Service Provider (ESP).

- The EVA is responsible for the administration on the EVs, including EVs' real identity registering, attribute allocation and private key generation. The EVA is also the central authority (CA) in Public Key Infrastructure (PKI) to publish AGGs' X.509 certification for secure channel establishment. Moreover, the EVA charges the electricity fees for the charging service on the EV according to the bill generated by AGG.

- The AGG provides multi-quality charging services to the EVs. There is unidirectional electricity flow from the AGG to the EVs. The AGG performs evaluation and authentication on the EV to determine its charging service quality and check its eligibility for charging service. The evaluation is based on a certain policy defined by AGG. Different AGGs in different default ESPs may have different policies. If the EV passes both evaluation and authentication, the EV can have QGS. If the EV

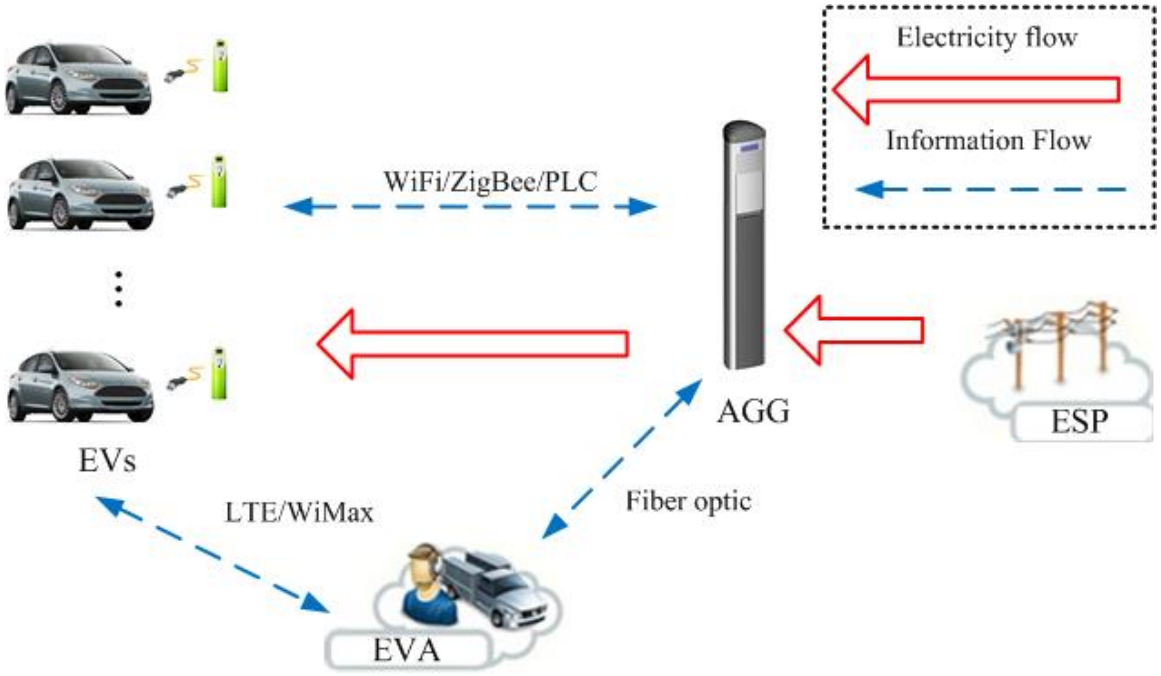

Figure 3.2: System Model in PMQC

only passes authentication, it can only have BES. Once the EV finishes charging, the AGG generates the EV's bill. With the EV's confirmation, the bill is transmitted to the EVA for fees charging on the corresponding EV's account.

- The EV can only charge power from the AGG. To have the charging service, the EV must be evaluated and authenticated by the AGG with its private key issued from EVA and stored in its non-reproducible storage.
- The ESP is the company to provide electricity. Each AGG has a belonging ESP. Each ESP may have multiple AGGs. The ESP provides the electricity resource to its AGGs. Specifically, there may be multiple ESPs in the V2G network.

The communication architecture is shown in Figure 3.2. The EVs can directly communicate with the EVA to synchronize the revocation list (RL). Cellular communication

techniques such as LTE and WiMax are deployed between the EVs and the EVA, due to the EVs' huge number and large scale mobility. To have charging service, the EV should park in the parking lot and have physical connection with the AGG. Thus various low cost communication techniques, such as WiFi, ZigBee and PLC can be implemented for communication between the EV and the AGG. Because of the remote and diverse distribution of the AGGs, also considering the heavy load on data transmission, fiber optic is a better choice for the communication between the AGG and the EVA.

3.2 Security Requirements

In the system model, the ESP is an electricity provider which does not participate in the interactions with the EVs. It is not involved in the EV's privacy-preservation issues. Thus, the ESP is not considered in the trust model. There are three entities in the trust model, EVA, AGG and EV.

- The EVA is a fully trusted entity. It has the full knowledge of all the EVs. This is reasonable since the EVA is normally established by a government authority.
- The AGG is honest but curious to the EV, which means it basically follows the protocol in the proposed scheme but tires its best to obtain as much private information of each EV as possible during interacting with the EV. Specifically, the private information for the EV includes its real identity, attribute, position and the EV owner's lifestyle.
- The EV is the entity whose privacy needs to be preserved. It is honest to all other entities. It can not maliciously modify, substitute or replay the messages to the AGG.

Based on the system model and trust model defined above, the goal in this thesis is to develop a privacy-preserving multi-quality charging scheme in V2G network. Specifically, the following four security requirements should be satisfied.

1. **Privacy Preservation:** The EV's attributes should not be obtained by AGG during the evaluation. Individual EV's real identity should not be disclosed to the AGG during the authentication. The EV owner's position and lifestyle privacy should not be deduced during the charging service.

2. **Fine-grained Access Control:** The AGG defines the access policy of the evaluation to determine which EV can have QGS. The access policy should be fine-grained. For example, "private vehicle" AND "priority service contract" OR "public vehicle" can have QGS. If and only if the EV's attributes satisfy the access policy can the EV have QGS.

3. **Traceability:** The EVA can trace the real identity of the EV according to the bill generated by AGG and confirmed by EV. After tracing the EV's real identity, corresponding electricity fees for the charging service can be charged on the EV's account. The EV can not deny the fees for the charging service either.

4. **Secure Revocation:** The EV's private key can be revoked by EVA. While revoking a EV's eligibility for charging, other EVs' eligibility and privacy should not be violated.

Chapter 4

Privacy-Preserving Multi-Quality Charging Scheme in V2G Network

In this chapter, the overview of the proposed privacy-preserving multi-quality charging (PMQC) scheme is introduced in Section 4.1. Then each phase of PMQC is explained in detail in Section 4.2.

4.1 Overview of the Proposed Scheme

The design goal of PMQC is to preserve the EV's attribute privacy, the EV owner's lifestyle and location privacy during the EV's interactions with the AGG. The ciphertext-policy attribute based encryption (CP-ABE) and group signature are utilized to achieve that goal. The interactions between the EV and the AGG are shown in Figure 4.1.

At the beginning, EV_k must be registered at the EVA with its real identity. The EVA allocates the attribute set S_k to EV_k, generates EV_k's private key SK_k and creates an account for EV_k to map its real identity with the corresponding private keys. Then EV_k obtains its private keys SK_k from the EVA secretly and stores it in its non-repudiable storage.

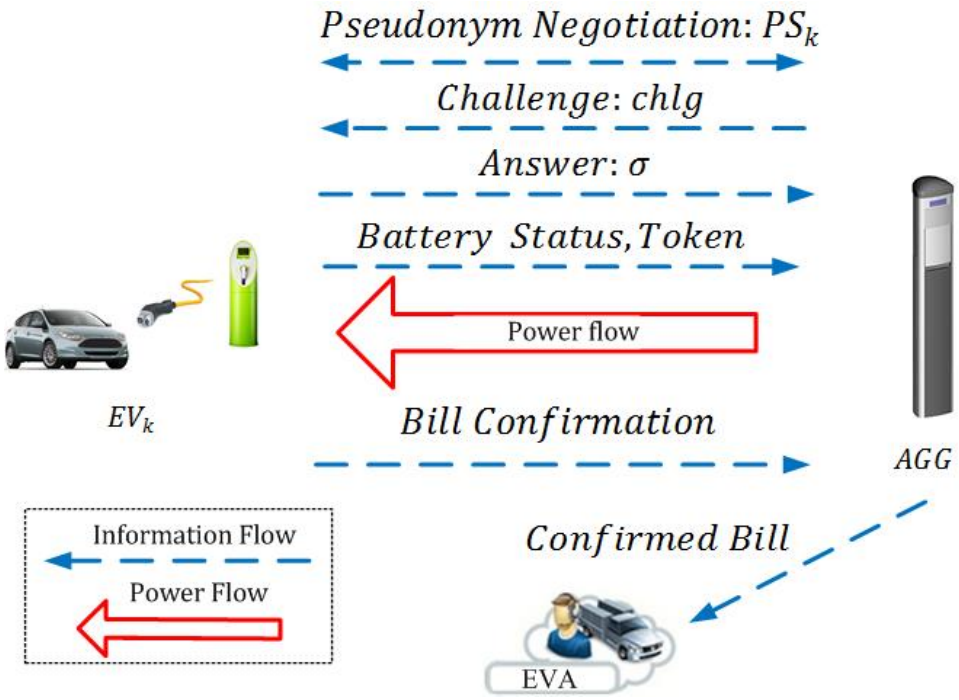

Figure 4.1: Interactions in PMQC

When EV_k connects to the AGG and requests for charging service, it first negotiates a pseudonym PS_k with the AGG to identify the session. Then the AGG performs service level evaluation and service eligibility authentication on EV_k to determine its charging service level and charging service eligibility.

To evaluate EV_k, the AGG randomly chooses two messages M_1 and M_2 for challenge. One is a plaintext, another one is a CP-ABE encrypted ciphertext based on the AGG's accessing policy $\mathbb{A}$. Then the challenge *chlg* is sent to EV_k. After receiving the challenge *chlg* from the AGG, EV_k decrypts the CP-ABE ciphertext on M_2. If the attribute set S_k in EV_k's private key SK_k matches the access poly $\mathbb{A}$ in the CP-ABE ciphertext, EV_k can successfully decrypt the CP-ABE ciphertext and obtain M_2, which means EV_k can have QGS from the AGG. Otherwise, EV_k can only have BES from the AGG.

In order to authenticate itself to the AGG, EV_k generates the group signature on M_1

and M_2 with its group signature private key GSK_k, which is a part of its private key SK_k. Then EV_k sends the group signature σ to the AGG. Otherwise, EV_k can only generate the group signature on M_1. After receiving the group signature σ from EV_k, the AGG verifies the group signature. If the received signature is based on both M_1 and M_2, EV_k can have QGS from the AGG. If the received signature is based on M_1, EV_k can only have BES from the AGG. If the group signature is invalid, EV_k's charging service request should be rejected.

The EV obtains the charging service from the AGG by providing tokens, which are hash values of a hash chain. Each token W_i indicates a certain amount of electricity. Fairness of the transaction between the EV and the AGG can be guaranteed under the token based mechanism. During the charging service, the AGG also has continuous monitoring on EV_k's battery status. EV_k periodically collects its battery status information, encrypts it with a shared symmetric key generated from the pseudonym PS_k, and sends the encrypted message to the AGG. The AGG may adjust the changing parameters based on the battery status monitoring information.

When the charging service completes, EV_k generates the group signature $\sigma_{W_{Last}}$ on the last token W_{Last} and sends them to the AGG, if EV_k expects to terminate the charging service. After receiving EV_k's group signature $\sigma_{W_{Last}}$, the AGG generates the signature $Sig_{AGG}(W_{Last})$ on the last token W_{Last} with its private key, and sends the last token W_{Last} with both two signatures to the EVA. The EVA checks $\sigma_{W_{Last}}$ and $Sig_{AGG}(W_{Last})$ to ensure both EV_k and the AGG confirm the charging service. Then the AGG traces EV_k's real identity from the group signature $\sigma_{W_{Last}}$. Finally, the corresponding electricity fees can be charged on EV_k's account.

4.2 Proposed PMQC Scheme

In this section, the proposed privacy-preserving multi-quality charging scheme (PMQC) for secure evaluation and authentication on the EV is formulated in detail. PMQC consists 6 phases: system initialization, service level evaluation, service eligibility authentication, battery monitoring, bill generation and revocation.

4.2.1 System Initialization

The EVA generates the key for each EV and AGG in this phase as shown in Figure 4.2. *Initl*{} is an arbitrary Bilinear Diffie-Hellman (BDH) parameter generator that satisfies the BDH assumption [56].

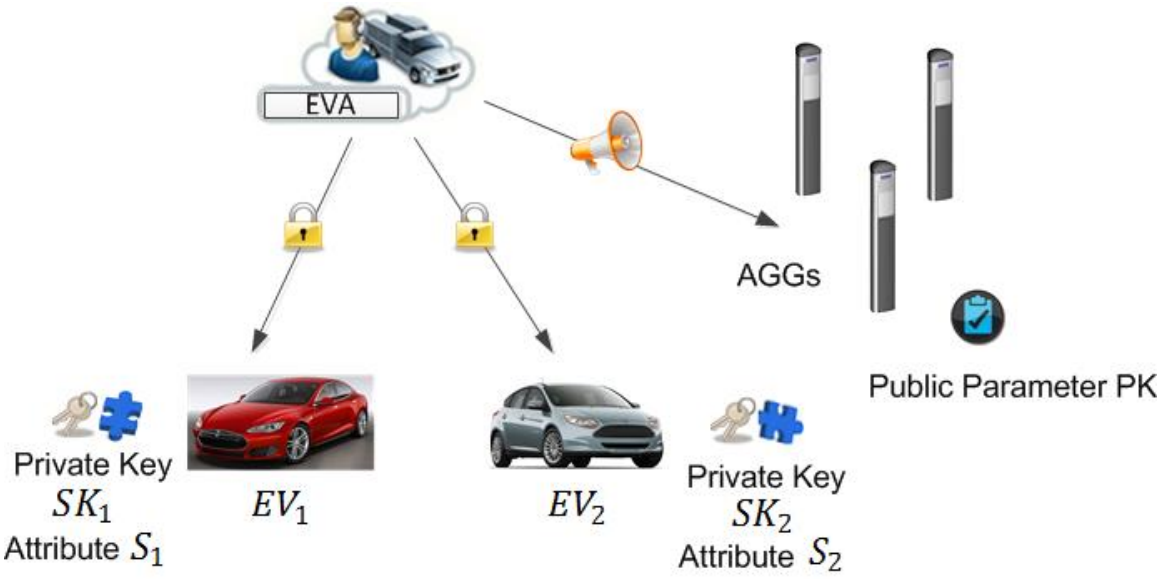

Figure 4.2: System Initialization in PMQC

- *Step-1*: The EVA is given a security parameter ψ to generate the bilinear parameters $\{p, g, \mathbb{G}, \mathbb{G}_T, e\}$ by running *Initl*$\{\psi\}$. g is the generator of group $\mathbb{G}$ with large prime order p. $\mathbb{G}$ and $\mathbb{G}_T$ form a bilinear map e: $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. The EVA chooses random exponents $\alpha, \varepsilon_1, \varepsilon_2 \in_R \mathbb{Z}_p^*$ and generates the master key:

$$MSK = (g^{\alpha}, \varepsilon_1, \varepsilon_2) \tag{4.1}$$

- *Step-2*: The EVA chooses random exponents $\beta, \gamma \in_R \mathbb{Z}_p^*$ and random group elements $h, q_1, q_2, \cdots, q_U \in_R \mathbb{G}$, where $q_1, q_2, \cdots, q_U$ are associated with the U attributes in this system. Then the EVA computes

$$f = g^{\beta} \tag{4.2}$$
$$\widetilde{e} = e(g,g)^{\alpha} \tag{4.3}$$
$$w = g^{\gamma} \tag{4.4}$$

and selects $u, v \in \mathbb{G}$ to satisfy

$$u^{\varepsilon_1} = v^{\varepsilon_2} = h \tag{4.5}$$

The EVA also finds four secure cryptographic hash functions

$$H_1 : \{0,1\}^* \rightarrow \mathbb{G} \tag{4.6}$$
$$H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_p^* \tag{4.7}$$
$$H_3 : \{0,1\}^* \rightarrow \{0,1\}^m \tag{4.8}$$
$$H_4 : \mathbb{Z}_p^* \rightarrow \{0,1\}^m \tag{4.9}$$

The EVA gets the group signature public key

$$GPK = (g, w) \tag{4.10}$$

and finally publishes public key:

$$PK = (GPK, h, u, v, f, \widetilde{e}, q_1 \cdots q_U, H_1 \cdots H_4) \tag{4.11}$$

- *Step-3*: When the AGG registers itself to the EVA, the AGG generates its public/private key pair pub_{AGG}/pvt_{AGG}. The EVA generates and publishes the AGG's X.509 certificate on its public key pub_{AGG} for secure channel establishment between the AGG and EV_k. The asymmetric encryption algorithm can be simple RSA algorithm.

- *Step-4*: When EV_k (k=1,2,...,m) registers itself to the EVA, it presents its identity ID_k to the EVA. Then the EVA allocates attribute set S_k to EV_k. The EVA chooses random exponent $t_k \in_R \mathbb{Z}_p^*$ for EV_k. Then it computes

$$D_k = g^{\alpha+\beta t_k} \tag{4.12}$$
$$D_k^{'} = g^{t_k} \tag{4.13}$$
$$D_{kx} = q_x^{t_k}, \forall x \in S_k \tag{4.14}$$

where x indicates one attribute of EV_k's attribute set S_k. Thus, the EVA gets the group signature private key

$$GSK_k = [\lambda_k = H_5(D_k), A_k = g^{1/(\gamma+\lambda_k)}] \tag{4.15}$$

Here $H_5 : \mathbb{G} \rightarrow \mathbb{Z}_p^*$ is a secure cryptographic hash functions. Finally the EVA loads the private key SK_k into EV_k's non-reproducible physical storage.

$$SK_k = (GSK_k, D_k, D_k^{'}, \forall x \in S_k : D_{kx}) \tag{4.16}$$

4.2.2 Service Level Evaluation

The AGG evaluates EV_k's attributes S_k to determine its service level as shown in Figure 4.3. Secure channel between EV_k and the AGG is established first. Then the AGG sends EV_k the challenge *chlg*, which is generated according to the AGG's access policy $\mathbb{A}$. By answering *chlg*, EV_k's attributes S_k associated with its private key SK_k can be evaluated.

Pseudonym Negotiation

EV_k and the AGG independently select random exponent $a, b \in_R \mathbb{Z}_p^*$. Then EV_k and the AGG exchanges g^a and g^b to negotiate the Diffie-Hellman sharing secret

$$g^{ab} = (g^a)^b = (g^b)^a \tag{4.17}$$

Based on the sharing secret, EV_k and the AGG can get the pseudonym

$$PS_k = H_4(g^{ab}) \tag{4.18}$$

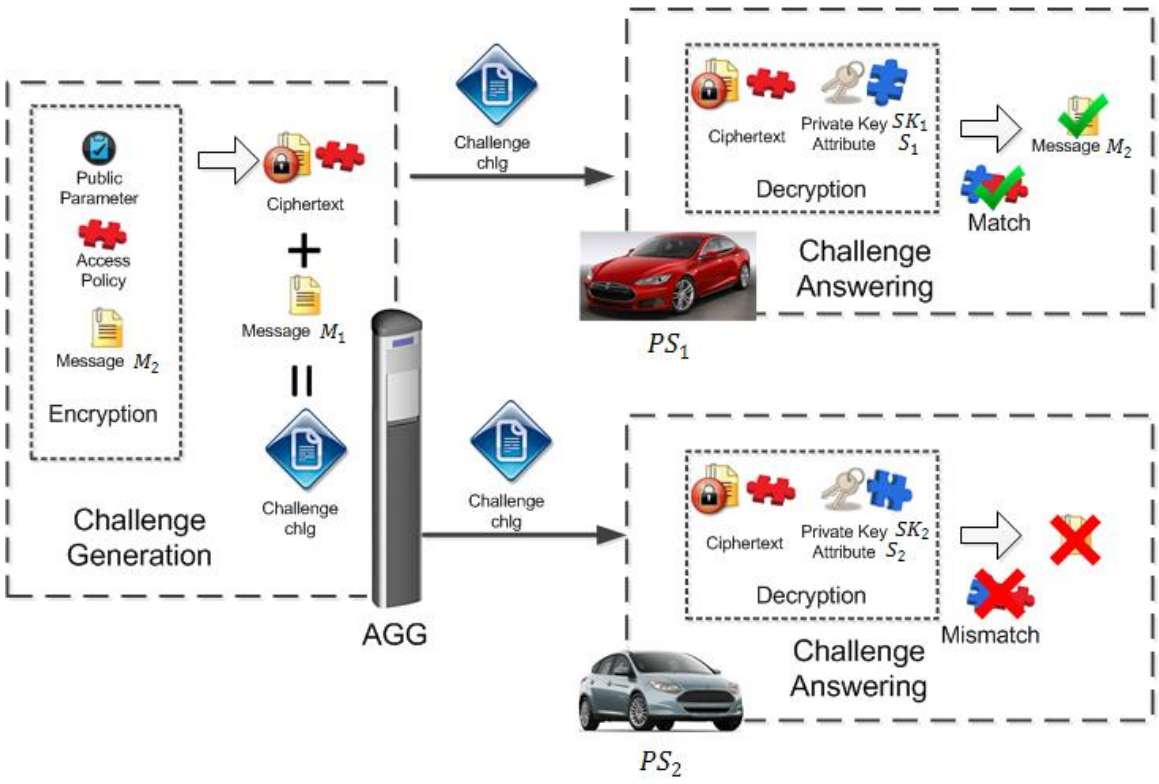

Figure 4.3: Service Level Evaluation in PMQC

The AGG associates all the following EV_k's interactions with pseudonym PS_k until EV_k checks out.

EV_k and the AGG independently select random exponent $a, b \in_R \mathbb{Z}_p^*$. Then EV_k and the AGG exchange g^a and g^b to negotiate the Diffie-Hellman sharing secret $g^{ab} = (g^a)^b = (g^b)^a$, and they generate the pseudonym $PS_k = H_4(g^{ab})$. The AGG associates all the interactions with pseudonym PS_k until EV_k checks out.

Challenge Generation

The AGG generates the challenge *chlg* to authenticate EV_k's eligibility, and evaluates EV_k's attributes S_k based the AGG's access policy $\mathbb{A}$ to determine its service quality. The AGG

chooses random messages $M_1, M_2 \in_R \{0,1\}^*$. Then the AGG performs ciphertext policy attribute based encryption [2] on M_2 to generate ciphertext

$$CT = Enc\{M_2, PK, [\mathbf{L}, \rho()]\} \tag{4.19}$$

$\mathbf{L}$ is a $l \times n$ Linear Secret-Sharing Schemes (LSSS) matrix pre-constructed according to the access policy $\mathbb{A}$. $\rho()$ is the function mapping rows of $\mathbf{L}$ to the attributes in S_k. The AGG first chooses random exponents $r_1, r_2, \cdots, r_l \in_R \mathbb{Z}_p^*$ and a random vector

$$\mathbf{y} = [s, y_2, y_3, \cdots, y_n]^T \in_R \mathbb{Z}_p^{*n} \tag{4.20}$$

Then for $j = 1$ to l the AGG computes

$$\varphi_j = \mathbf{l}_j \cdot \mathbf{y} \tag{4.21}$$

where vector $\mathbf{l}_j$ is the jth row of the LSSS matrix $\mathbf{L}$.

The ciphetext CT can be generated:

$$\begin{aligned} CT = [&C = M_2 \tilde{e}^s, C^{'} = g^s, (C_1 = f^{\varphi_1} q_{\rho(1)}^{-r_1}, C_1^{'} = g^{r_1}), \\ &\cdots, (C_l = f^{\varphi_l} q_{\rho(l)}^{-r_l}, C_l^{'} = g^{r_l}), \mathbf{L}, \rho()] \end{aligned} \tag{4.22}$$

Then the AGG sends the challenge

$$chlg = \{M_1, CT, TS, Sig_{AGG}[H_3(M_1 \parallel CT \parallel TS)]\} \tag{4.23}$$

to EV_k, where TS is the time stamp, $Sig_{AGG}[H_3(M_1 \parallel CT \parallel TS)]$ is the signature signed by AGG with its private key pvt_{AGG}.

Challenge Answering

After receiving *chlg* from the AGG, EV_k first verifies its integrity. Then it decrypts the ciphertext CT. If EV_k can successfully decrypt CT in *chlg* to obtain M_2, EV_k is able to have the QGS. Otherwise, EV_k can only have the BES. EV_k decrypts the ciphertext CT by the following steps:

- *Step-1*:EV_k computes the subset $J_k \subseteq J$ satisfying

$$\{\rho(j) : j \in J_k\} \subseteq S_k \tag{4.24}$$

  where J is the set of row index of matrix $\mathbf{L}$ and j indicates the index of jth row in matrix $\mathbf{L}$. If EV_k's attributes S_k matches the access structure $\mathbb{A}$ in matrix $\mathbf{L}$, there would be a set of constant $\{\omega_j \in \mathbb{Z}_p^* : j \in J_k\}$ satisfying

$$\sum_{j \in J_k} \omega_j \cdot \mathbf{l}_j = (1, 0, \cdots, 0) \tag{4.25}$$

  Specifically,

$$\sum_{j \in J_k} \omega_j \cdot \varphi_j = \sum_{j \in J_k} \omega_j \cdot \mathbf{l}_j \cdot \mathbf{y} = (\sum_{j \in J_k} \omega_j \cdot \mathbf{l}_j) \cdot \mathbf{y} = s \tag{4.26}$$

  Otherwise, such set of number does not exist. The ciphertext CT can not be decrypted.

- *Step-2*:If such set of constant $\{\omega_j \in \mathbb{Z}_p^* : j \in J_k\}$ can be found, EV_k decrypts the ciphertext CT to obtain M_2:

$$
\begin{aligned}
\hat{C} &= \frac{e(C', D_k)}{\prod_{j \in J_k} [e(C_j, D'_k) \cdot e(C'_j, D_{k\rho(j)})]^{\omega_j}} \\
&= \frac{e(g,g)^{\alpha s} \cdot e(g,g)^{s\beta t_k}}{\prod_{j \in J_k} e(g,g)^{\beta \varphi_j \omega_j t_k}} \\
&= \frac{e(g,g)^{\alpha s} \cdot e(g,g)^{s\beta t_k}}{e(g,g)^{\beta t_k \sum_{j \in J_k} \varphi_j \omega_j}} \\
&= \frac{e(g,g)^{\alpha s} \cdot e(g,g)^{s\beta t_k}}{e(g,g)^{s\beta t_k}} \\
&= e(g,g)^{\alpha s}
\end{aligned}
\tag{4.27}
$$

$$
M_2 = C / \hat{C} = M_2 \cdot e(g,g)^{\alpha s} / e(g,g)^{\alpha s} \tag{4.28}
$$

4.2.3 Service Eligibility Authentication

After the service level evaluation, EV_k responses to the AGG to authenticate itself with the group signature [49] on the messages $M1$ and $M2$ in *chlg*. If the group signature can be verified by the AGG, EV_k has the eligibility for the charging service. The detail of this phase is shown in Figure 4.4.

Authentication Answering

EV_k generates the group signature on the message M as an authentication answer to the AGG. The message M for EV_k to sign is $M = M_1 \parallel M_2$ if CT is decrypted, otherwise it is $M = M_1$. The group signature can be generated by the following steps:

- *Step-1*: EV_k chooses random exponents $\mu, \nu, r_\mu, r_\nu, r_{\lambda_k}, r_{\delta_1}, r_{\delta_2} \in_R \mathbb{Z}_p^*$ and computes

$$
\delta_1 = \lambda_k \mu \tag{4.29}
$$

$$
\delta_2 = \lambda_k \nu \tag{4.30}
$$

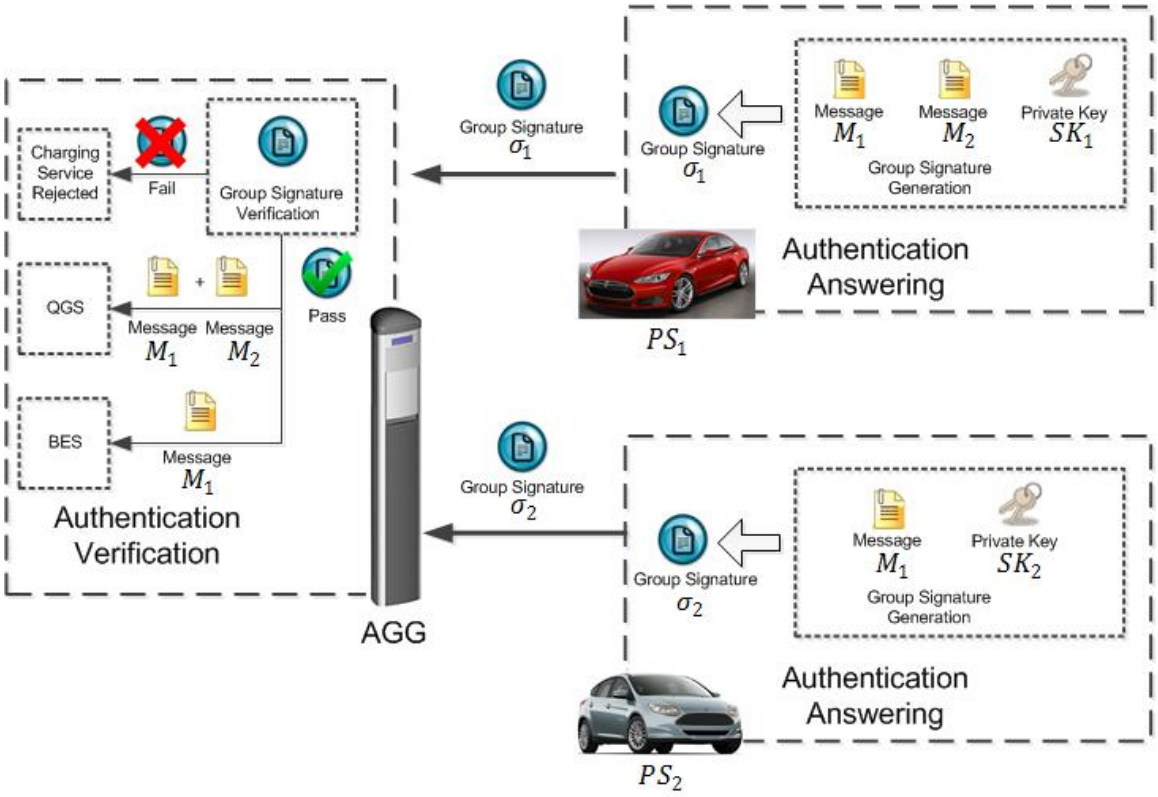

Figure 4.4: Service Eligibility Authentication in PMQC

- *Step-2*: EV_k computes hash c on message M.

$$c = H_2(M \parallel T_1 \parallel T_2 \parallel T_3 \parallel R_1 \parallel R_2 \parallel R_3 \parallel R_4 \parallel R_5) \tag{4.31}$$

$$\begin{aligned} &T_1 = u^{\mu}, T_2 = v^{\nu}, T_3 = A_k h^{\mu+\nu} \\ &R_1 = u^{r_\mu}, R_2 = v^{r_\nu}, R_4 = T_1^{r_{\lambda_k}} \cdot u^{-r_{\delta_1}}, R_5 = T_2^{r_{\lambda_k}} \cdot v^{-r_{\delta_2}} \\ &R_3 = e(T_3, g) \cdot e(h, w)^{-r_\mu - r_\nu} \cdot e(h, g)^{-r_{\delta_1} - r_{\delta_2}} \end{aligned} \tag{4.32}$$

- *Step-3*: EV_k computes the group signature σ on message M. Then EV_k sends it to the AGG.

$$\sigma = (T_1, T_2, T_3, c, t_\mu, t_\nu, t_{\lambda_k}, t_{\delta_1}, t_{\delta_2}) \tag{4.33}$$

where $t_\mu = r_\mu + c\mu, t_\nu = r_\nu + c\nu$, $t_{\lambda_k} = r_{\lambda_k} + c\lambda_k$, $t_{\delta_1} = r_{\delta_1} + c\delta_1, t_{\delta_2} = r_{\delta_2} + c\delta_2$.

Authentication Verifying

The AGG verifies the group signature received from EV_k. If the group signature on $M = M_1 \parallel M_2$ is verified, EV_k can have QGS. If the group signature on $M = M_1$ is verified, EV_k can only have BES. If the group signature is invalid, EV_k's charging service request should be rejected. The verification steps are below:

- *Step-1*:AGG computes:

$$\begin{aligned} \tilde{R}_1 = u^{t_\mu} \cdot T_1^{-c}, \tilde{R}_2 = v^{t_\nu} \cdot T_2^{-c} \\ \tilde{R}_4 = T_1^{t_{\lambda_k}} \cdot u^{t_{\delta_1}}, \tilde{R}_5 = T_2^{t_{\lambda_k}} \cdot v^{t_{\delta_2}} \end{aligned} \tag{4.34}$$

$$\begin{aligned} \tilde{R}_3 = e(T_3, g)^{t_{\lambda_k}} \cdot e(h, w)^{-t_\mu - t_\nu} \cdot \\ e(h, g)^{-t_{\delta_1} - t_{\delta_2}} \cdot [e(T_3, w)/e(g, g)]^c \end{aligned} \tag{4.35}$$

- *Step-2*:AGG checks:

$$c \stackrel{?}{=} H_2(M \parallel T_1 \parallel T_2 \parallel T_3 \parallel \widetilde{R}_1 \parallel \tilde{R}_2 \parallel \tilde{R}_3 \parallel \tilde{R}_4 \parallel \tilde{R}_5) \tag{4.36}$$

4.2.4 Battery Monitoring

After confirming EV_k's service level and eligibility, the AGG provides QGS or BES to EV_k as shown in Figure 4.5, which are both under the AGG's monitoring. To maintain the fairness of the transaction between EV_k and the AGG, a charging service mechanism based on hash chain is utilized [57]. EV_k takes the multi-quality charging service from the AGG according to the following steps:

- *Step-1*: If the EV_k expects KH units of electricity from the AGG, it sends its electricity demand and its pseudonym $\{KH, PS_k\}$ to the EVA through secure channel.

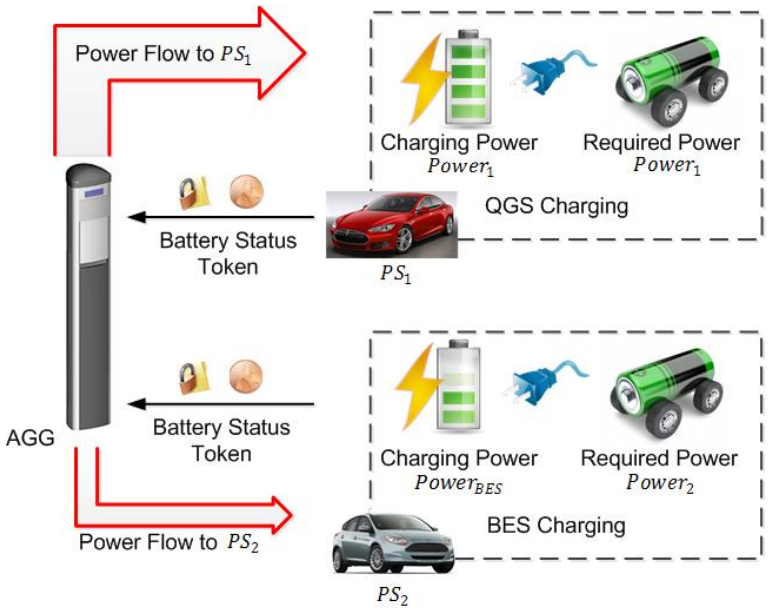

Figure 4.5: Multi-Quality Charging in PMQC

- *Step-2*: The EVA randomly selects a message $W_{KH} \in \{0,1\}^*$. Then it creates a hash chain, $W_0, W_1, \cdots, W_{KH}$, with the hash chain root W_{KH}, which satisfies

$$W_i = H_3(W_{i+1}), (i = KH-1, KH-2, \cdots, 0) \tag{4.37}$$

  W_0 is the final hash value of the hash chain. Each element W_i can be regarded as a token, which indicates one unit of electricity during the charging service. After computing the hash chain, the EVA sends the message $\{KH, W_{KH}, W_0\}$ to EV_k through secure channel. In addition, the EVA also sends the message $\{PS_k, KH, W_0\}$ to the AGG through secure channel.

- *Step-3*: After receiving the message from the EVA, EV_k and the AGG independently generate a shared symmetric key based on the pseudonym PS_k at first. EV_k restores the whole hash chain from the root W_{KH} to the final value W_0 by computing $W_i = H_3(W_{i+1}), (i = KH-1, KH-2, \cdots, 0)$. Then EV_k encrypts its current battery status BS_1 and the token W_1 into the symmetric ciphertext $E_{PS_k}(BS_1, W_1)$ and

sends it to the AGG. The AGG verifies the token by comparing the hash value of the token $H_3(W_1)$ with W_0.

$$W_0 \stackrel{?}{=} H_3(W_1) \tag{4.38}$$

If the token W_1 from EV_k can be verified, the AGG sets proper charging parameter according to EV_k's battery status BS_1 and provides one unit of electricity to EV_k.

- *Step-4*: EV_k and the AGG repeat the latter part of step-3 with token W_i by verifying

$$W_i \stackrel{?}{=} H_3(W_{i+1}) \tag{4.39}$$

until EV_k finishes all KH units charging or EV_k departs before its battery being fully charged. At the last charging interaction, EV_k generates a group signature $\sigma_{W_{Last}}$ on the token of the last charging interaction W_{Last}. W_{Last} can be W_{KH} or any other token before W_{KH}. Then EV_k sends $E_{PS_k}(BS_{Last}, W_{Last}, \sigma_{W_{Last}})$ as the last charging request to the AGG.

4.2.5 Bill Generation

After completing the charging service, the EVA generates EV_k's bill and charges the electricity fees by the following steps:

- *Step-1*: The AGG generates a signature $Sig_{AGG}(W_{Last})$ on the last token from EV_k with its private key to indicate its confirmation. Then the AGG sends its signature $Sig_{AGG}(W_{Last})$, EV_k's group signature $\sigma_{W_{Last}}$ and the last token W_{Last} to the EVA.
- *Step-2*: The EVA checks the integrity by verifying both $Sig_{AGG}(W_{Last})$ and $\sigma_{W_{Last}}$, in order to make sure that both AGG and EV_k confirm this charging service. Then the EVA calculates the fees for EV_k's charging service according to its last token W_{Last} sent to the AGG.

- *Step-3*: The EVA tracks EV_k's real identity from the group signature $\sigma_{W_{Last}}$ by obtaining A_k in EV_k's group signature private key GSK_k. The EVA computes

$$A_k = T_3/(T_1^{\varepsilon_1} \cdot T_2^{\varepsilon_2}) \tag{4.40}$$

with the group signature master key $GMSK = (\varepsilon_1, \varepsilon_2)$, and tracks its identity ID_k by looking up the user index. Then the EVA charges the electricity fees on ID_k's account.

4.2.6 Revocation

Each EV or AGG maintains a revocation list

$$RL = \{GSK_1, GSK_2 \cdots, GSK_r, date\} \tag{4.41}$$

which includes the revoked EVs' group signature private keys and the issuing date. If the EVA wants to revoke $EV_{r+1}, EV_{r+2} \cdots, EV_{r+m}$, it adds their group signature private keys and publishes the new

$$RL' = \{GSK_1, GSK_2 \cdots, GSK_r, GSK_{r+1}, GSK_{r+2} \ldots, GSK_{r+m}, date'\} \tag{4.42}$$

to the public in any necessary time.

Once received the new RL', the unrevoked EVs and the AGGs update their private keys and public keys immediately, according to the newly added items in the RL'. EV_k updates its group signature private key GSK_k as Algorithm 1:

The AGG updates its group signature public key GPK as Algorithm 2:

$A_k^{(i)}$ indicates the ith updating for A_k, $A_k^{(m)}$ is the final output of the algorithms, specifically $A_k = A_k^{(0)}$. Such rule also applies to $g^{(i)}$ and $w^{(i)}$.

Algorithm 1 EV_k's group signature private key revocation

Input: $GSK_{r+1}, \ldots GSK_{r+m}, GSK_k = (A_k, \lambda_k)$;

Output: $GSK_k^{(m)} = (A_k^{(m)}, \lambda_k)$;

1: **for** each $i = 1$ to m **do**
2: $\quad A_k^{(i)} = \frac{[A_{r+i}^{(i-1)}]^{1/(\lambda_k - \lambda_{r+i})}}{[A_k^{(i-1)}]^{1/(\lambda_k - \lambda_{r+i})}}$;
3: $\quad$ **for** each $j = i + 1$ to m **do**
4: $\quad\quad A_{r+j}^{(i)} = \frac{[A_{r+i}^{(i-1)}]^{1/(\lambda_{r+j} - \lambda_{r+i})}}{[A_{r+j}^{(i-1)}]^{1/(\lambda_{r+j} - \lambda_{r+i})}}$;
5: $\quad$ **end for**
6: **end for**

Algorithm 2 The AGG's group signature public key revocation

Input: $GSK_{r+1}, \ldots GSK_{r+m}, GPK = (g, w)$;

Output: $GPK^{(m)} = (g^{(m)} w^{(m)})$;

1: **for** each $i = 1$ to m **do**
2: $\quad g^{(i)} = A_{r+1}^{(i-1)}$;
3: $\quad w^{(i)} = g^{(i-1)} \cdot ({A_{r+i}}^{(i-1)})^{-\lambda_{r+i}}$;
4: $\quad$ **for** each $j = i + 1$ to m **do**
5: $\quad\quad A_{r+j}^{(i)} = \frac{[A_{r+i}^{(i-1)}]^{1/(\lambda_{r+j} - \lambda_{r+i})}}{[A_{r+j}^{(i-1)}]^{1/(\lambda_{r+j} - \lambda_{r+i})}}$;
6: $\quad$ **end for**
7: **end for**

Chapter 5

Security Analysis and Performance Evaluation

In this chapter, the security analysis on PMQC is performed in Section 5.1. Section 5.2 is about the performance evaluation on PMQC.

5.1 Security Analysis

Under the trust model defined in Section 3.2, the security properties of PMQC are analyzed in this section. The security analysis demonstrates that PMQC satisfies all the security requirements in Section 3.2.

5.1.1 Privacy-Preservation

The real identity and attributes of the EV are kept confidential to the AGG, which provides the multi-quality charging service to the EVs. Because the full-anonymity is achieved in the group signature[49], the AGG can check the EV's service eligibility without knowing the EV's real identity by verifying the group signature. All the interactions between the EV and the AGG are linked to the pseudonym, which is negotiated between the EV and the

AGG based on the sharing Diffie-Hellman secret. Thus, the real identity of the EV can be kept secret during all the interactions with the AGG. In addition, the AGG can not obtain the EV's attributes during the evaluation, since the attributes are in the EV's private key. Furthermore, the EV can confirm its charging bill to the AGG without revealing its real identity by signing a group signature on it. By opening this group signature with the group signature master key, the EVA can track the real identity of the EV, which signs the group signature, and charges corresponding fees for charging service on this EV's account. As a result, real identity-hidden fees charging is achieved. Lastly, by hiding EV's real identity, the AGG can hardly relate the location of the EV and the battery status monitoring information with the EV owner. Thus the EV owner's location and life style privacy are also preserved.

5.1.2 Fine-grained Access Control

The AGG defines the access policy of the evaluation, builds corresponding LSSS matrix and generates the challenge. The access policy expressed by the LSSS matrix supports both "AND" and "OR" gates[2]. The AGG sends a challenge to the EV, which includes a ciphertext-policy attribute based encryption (CP-ABE) ciphertext generated according to the access policy, in order to evaluate the EV's attributes. If and only if the EV's attributes in its private key match the AGG's access policy in the CP-ABE ciphertext CT, can the EV decrypt the CP-ABE ciphertext and answer the challenge. Thus, the fine-grained access control on the qualified EVs for QGS is achieved in PMQC.

5.1.3 Traceability

After the charging service, the AGG sends the bill to the EV. The EV generates the group signature on the bill issued by AGG to indicate its confirmation on the bill. Both AGG and EVA can check the confirmation by verifying the group signature. In addition, because the full-traceability is achieved in the group signature[49], the EVA can track the real identity of the EV by opening the group signature with the group signature master key. Obtaining the real identity of the EV, corresponding electricity fees can be charged on the

EV's account. Also, the EV can hardly deny its electricity fees for the charging service, because of the non-repudiation achieved by the group signature.

5.1.4 Secure Revocation

The EVA can revoke any EV by publishing its group signature private key to the RL at any time. The revoked EV loses its service eligibility after the AGG updates the group signature public key. The unrevoked EVs' eligibilities are not effected after they update their group signature private keys. If the revoked EV wants to regain the service eligibility, it should return to the EVA to re-register. If its re-registering is successful, the EVA formats the EV's non-reproducible physical storage and writes a new private key with a new group signature private key. The EV's attributes can also be updated during the new private key issuing process. Because the new group signature private key is unrelated to the revoked group signature private key, the EV's identity can be kept confidential when it regains charging service eligibility.

5.2 Performance Evaluation

In this section, performance evaluation is performed in terms of security feature as well as computation overhead and communication overhead.

5.2.1 Security Features

Security features are compared among the proposed scheme PMQC, Yang's scheme and Liu's scheme in Table 5.1. All the schemes realize identity-hidden authentication, which means the EV can be authenticated by AGG without revealing its real identity. Yang's scheme and PMQC consider the revocation problem. Yang's scheme revokes the EV by simply setting a expiry date. The EV cannot be dynamically revoked at any necessary time. In contrast, the EVA that manages all the EVs can revoke any EV at any necessary time in PMQC. Specifically, the EVA publishes the revoked EV's private key to the revocation

Table 5.1: Comparison of the Security Features

	Liu's[25]	Yang's[22]	PMQC
ID-hidden authentication	√	√	√
Secure Revocation	×	√	√
Attribute-hidden evaluation	×	×	√
ID-hidden bill generation	×	×	√

list in each AGG or each EV. Once received the new revocation list, the AGG and the unrevoked EV update their keys. After the update, the revoked EV can no longer have the charging service eligibility. Any other unrevoked EV's charging service eligibility is not effected, its privacy is not violated either. In addition, PMQC realizes attribute-hidden evaluation and identity-hidden bill generation, which are not achieved in the other two schemes. Based on the attribute-hidden evaluation, the AGG can determine the charging service quality to the EV without violating its attribute privacy. The AGG can generate the EV's charging service bill for the EVA to charge fees on the EV's account without revealing the EV's real identity.

5.2.2 Computation Overhead

The computation overhead of authentication and verification in PMQC are compared with that in Yang's scheme. Compared with the pairing operation, exponentiation operation in $\mathbb{G}$ and exponentiation operation in $\mathbb{G}_T$, other operations are negligible[58]. Let T_P be the time for a pairing operation, T_e be the time for an exponentiation operation in $\mathbb{G}$, and T_{eT} be the time for an exponentiation operation in $\mathbb{G}_T$.

In the *Authentication* phase, there are 9 exponentiation operations in $\mathbb{G}_T$ and 8 pairing operations in Yang's scheme, which cost $9\,T_{eT} + 8\,T_P$ in total. Even though PMQC has 11 exponentiation operations in $\mathbb{G}$, there are only 1 exponentiation operation in $\mathbb{G}_T$ and only 2 time consuming pairing operations. The total computation overhead in PMQC is $11\,T_e + 1\,T_{eT} + 3\,T_P$.

Table 5.2: Notations in the Computation Overhead Evaluation of PMQC

Symbols	Meanings
T_P	Time for a pairing operation
T_e	Time for an exponentiation operation in $\mathbb{G}$
T_{eT}	Time for an exponentiation operation in $\mathbb{G}_T$

In the *Verification* phase, 5 exponentiation operations in $\mathbb{G}_T$ and 6 pairing operations need to be performed in Yang's scheme, which cost $5T_{eT} + 6T_P$. In contrast, PMQC has much less time cost in verification phase, which is $9T_e + 3T_{eT} + 2T_P$.

In addition, the simulations are conducted on a computer with a 3.0 GHz processor and 1 GB memory under MIRACL library[59]. A pairing operation, an exponentiation operation in $\mathbb{G}_T$ and an exponentiation operation in $\mathbb{G}$ cost $4.5ms$, $2.3ms$ and $0.6ms$. Figure 5.1 and Figure 5.2 show that PMQC can achieve lower computation overhead for both authentication and verification.

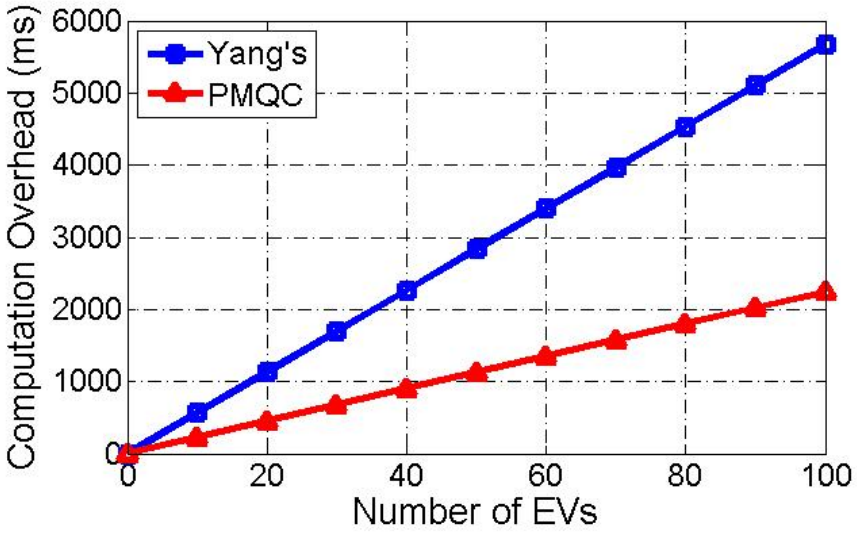

Figure 5.1: Comparison of the Computation Overhead in Authentication

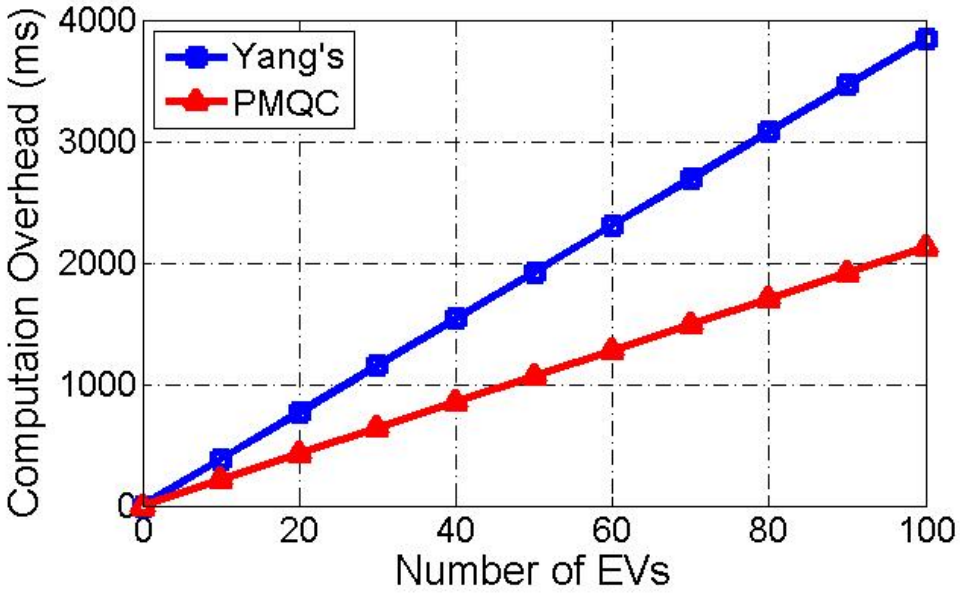

Figure 5.2: Comparison of the Computation Overhead in Verification

5.2.3 Communication Overhead

Most of the communication overhead in PMQC comes from the AGG's periodical monitoring on the EV's battery status during charging. The periodical monitoring information can be carried by a very short message, which is no larger than 100 bytes. The period of reporting is usually several or tens of seconds[13]. Thus, the communication overhead between the EV and the AGG in PMQC is very low. Low cost communication techniques such as WiFi, ZigBee and PLC are suitable for the low communication overhead scenario.

Chapter 6

Extended Privacy-Preserving Multi-Quality Charging Scheme in V2G Network

Based on the proposed PMQC in Chapter 4, the extended privacy-preserving multi-quality charging (ePMQC) scheme in V2G network is proposed in this chapter. The extended system model of ePMQC is defined in Section 6.1. Then each phase of ePMQC is formulated in Section 6.2. Section 6.3 is about the performance enhancement of ePMQC compared with PMQC.

6.1 Extended System Model

In PMQC, the AGG evaluates each EV to determine its charging service quality based on its attributes. However, if the AGG accepts too many EVs for QGS, some problems may arise.

- First of all, the charging power for the BES EVs varies according to the remaining power in the AGG after guaranteeing the charging power of all the QGS EVs. The

total power that the AGG can provide is limited. The more QGS EVs in the AGG, the less total power can be provided for BES EVs. If too much power in the AGG is consumed by the QGS EVs, the charging power for the BES EVs may be very low. Thus, the charging service quality for the BES EVs is seriously effected in such a scenario. In the worst case, the BES EVs can not have charging service, since all the power that the AGG can provide is allocated to the large number of QGS EVs.

- Second, besides providing charging service to the EVs, the V2G network should provide regulation service to the power grid. Due to the unidirectional electricity flow in the V2G network, the V2G work provides regulation service to the power grid by adjusting the power that it consumes from the power grid. Specifically, if the power grid is in electricity shortage during the peak load hours, the V2G network can reduce its power consumption from the power grid by lowering the power for BES EVs, in order to reduce the peak load of the power grid. Consequently, the total power of each AGG in V2G network for charging service should decrease. However, the capacity of the regulation service that the V2G network can provide is constrained by the number of QGS EVs under charging. Since the charging power for the QGS EVs should be guaranteed, the minimum power that the AGG has to consume from the power grid is the summation of all its QGS EVs' charging power. The more QGS EVs are there in the AGG, the higher minimum power the AGG has to consume. If there are too many QGS EVs in the AGGs, the power that the V2G network consumes from the power grid can hardly be significantly reduced. Thus, the capacity of the V2G network to provide regulation service to the power grid is very low.

As a result, the total number of QGS EVs should be strictly controlled in a single AGG. However, the AGG may be unwilling to limit the number of QGS EVs. The AGG is belonged to a certain ESP, which is a company trying its best to maximize the profit. Because the service fee for QGS is much higher than that for BES, the AGG always tries its best to enroll as many QGS EVs as possible in order to maximize the profit. It is contradictory that the AGG is willing to control the total number of QGS EVs, which may reduce the AGG's profit. To this end, the Independent System Operator (ISO), which is a non-profit institution with the responsibility to maintain the regulation service capacity

and the overall stability of the V2G network, is introduced to audit on the EV's charging request in order to control the number of QGS EVs in a single AGG. If and only if the EV provides the permission from the ISO to the AGG and passes the AGG's evaluation, can the EV have QGS from the AGG. While maintaining the regulation service capacity and the overall stability of V2G network, the ISO also relieves the computation overhead on the EV, which usually has very limited computation capability and storage capacity. The system model and trust model should be modified due to the introduction of the new entity ISO. Based on the system model and the trust model of PMQC in Chapter 3, extended system model for ePMQC is shown in Figure 6.1.

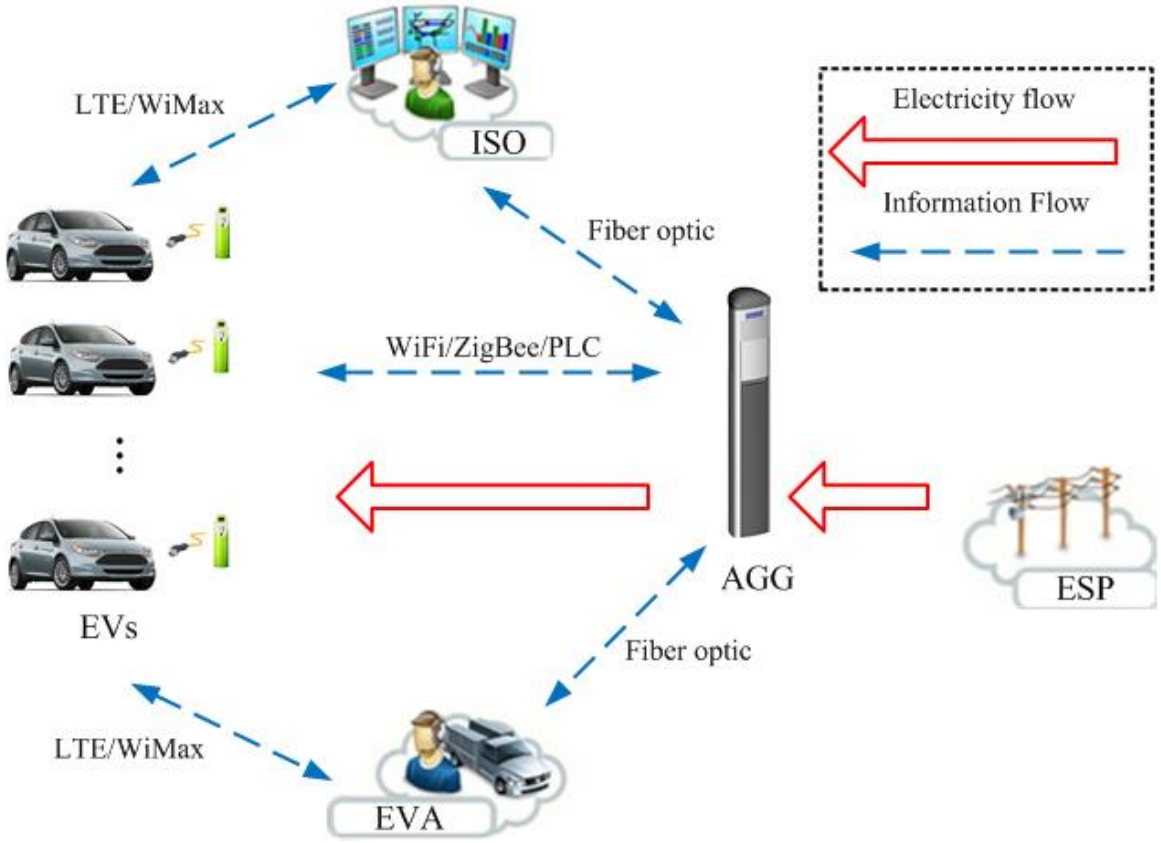

Figure 6.1: Extended System Model in ePMQC

- The responsibility of the ISO is to audit the EV's charging request. Specifically, the ISO controls the total number of QGS EVs in a single AGG by issuing permissions to the EVs that request for charging service. If there are too many EVs in a single AGG, the ISO may stop issuing permissions to the new incoming EVs for QGS in that AGG, no matter the EVs pass the AGG's evaluation or not.

- The ISO is a non-profit institution to maintain the regulation service capacity and the overall stability of the V2G network. It can hardly obtain any interest from violating the EV's privacy. For this reason, the ISO is a semi-trusted entity to both AGG and EV in the trust model of ePMQC.

6.2 Proposed ePMQC Scheme

There are 7 phases in ePMQC including system initialization, service level evaluation, service request auditing, service eligibility authentication, battery monitoring, bill generation and revocation.

The difference between PMQC and ePMQC is that a service request auditing phase is added in ePMQC. Specifically, the EVA does not directly send the evaluation challenge to the EV to evaluate its attributes and determine its service level. Instead, the EVA sends the evaluation challenge to the ISO for auditing. The ISO audits the EV's charging service request by pre-decrypting the CP-ABE ciphertext in the evaluation challenge with the temperate key received from the EV, which is generated by the EV based on its private key. The temperate key contains all the EV's attributes. If the attributes in the temperate key match the access control policy in the CP-ABE ciphertext in the evaluation challenge, the ISO can successfully pre-decrypt the CP-ABE ciphertext. If the ISO successfully pre-decrypts the CP-ABE ciphertext and grants the EV's request for QGS, a permission with the pre-decryption result is sent to the EV. Thus, the EV passes the AGG's evaluation and the ISO's auditing to have QGS. On the other hand, if the ISO fails to pre-decrypt the CP-ABE ciphertext due to the mismatch between the EV's attributes and the AGG's access control policy, or if the ISO prohibits the AGG to accept more QGS EVs, the ISO sends a permission without the pre-decryption result to the EV. As a result, the EV can

only have BES. The interactions between the EV , the ISO and the AGG are shown in Figure 6.2.

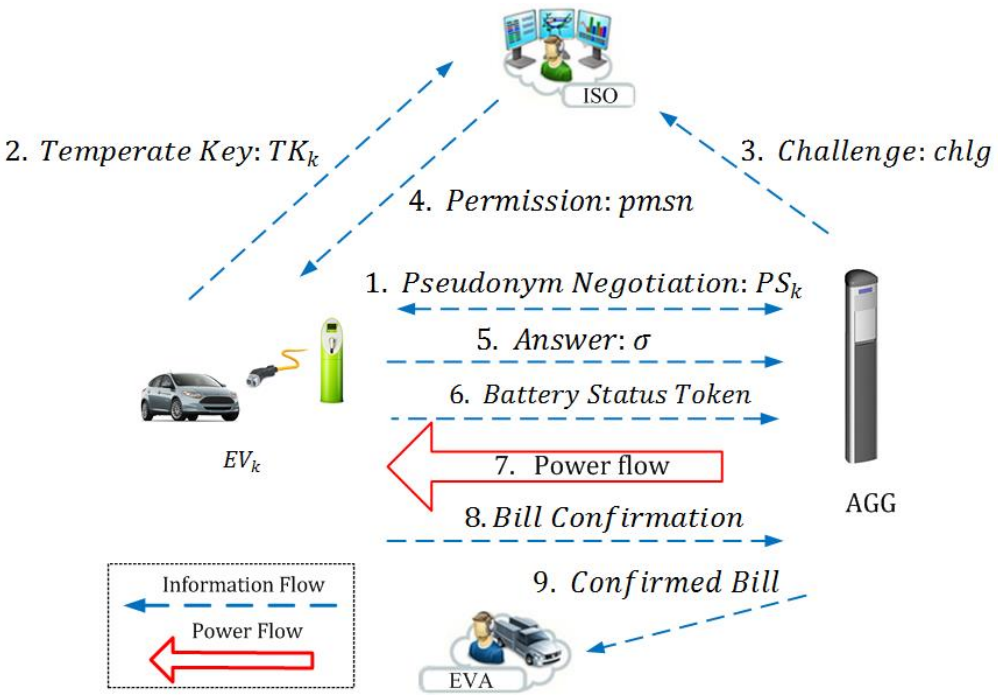

Figure 6.2: Interactions in ePMQC

6.2.1 System Initialization

The system initialization phase in ePMQC is the same as that in PMQC as shown in subsection 4.2.1. The EVA generates the master key MSK and keeps it secretly.

$$MSK = (g^{\alpha}, \varepsilon_1, \varepsilon_2) \tag{6.1}$$

The EVA publishes its public key PK, the AGG's public key pub_{AGG} with corresponding X.509 certificate, and the ISO's public key pub_{ISO}.

$$GPK = (g, w) \tag{6.2}$$
$$PK = (GPK, h, u, v, f, \tilde{e}, q_1 \cdots q_U, H_1 \cdots H_4) \tag{6.3}$$

The EVA generates EV_k's private key SK_k associated with the attribute set S_k, and sends it to EV_k through secure channel. EV_k stores the received private key in its non-reproducible storage.

$$GSK_k = (\lambda_k, A_k) \tag{6.4}$$
$$SK_k = (GSK_k, D_k, D_k^{'}, \forall x \in S_k : D_{kx}) \tag{6.5}$$

Specifically,

$$D_k = g^{\alpha+\beta t_k} \tag{6.6}$$
$$D_k^{'} = g^{t_k} \tag{6.7}$$
$$D_{kx} = q_x^{t_k}, \forall x \in S_k \tag{6.8}$$

6.2.2 Service Level Evaluation

In this phase, the pseudonym PS_k is negotiated first between the AGG and EV_k to identify the charging service session. Then, the EV_k generates a a temperate key TK_k based on its private key SK_k, and sends it with the pseudonym PS_k to the ISO for auditing. Meanwhile, the AGG generates the challenge *chlg* based on the AGG's access policy $\mathbb{A}$ in order to evaluate EV_k's attributes for QGS. The AGG also sends the challenge *chlg* with the pseudonym PS_k to the ISO for auditing.

Pseudonym and Temperate Key Generation

The EVA and the AGG negotiate the pseudonym in the same way as that in PMQC to get the pseudonym PS_k. Then EV_k chooses a random exponent $\theta \in_R \mathbb{Z}_p^*$ and generates a temperate key TK_k based on its private key SK_k.

$$\begin{aligned} TD_k &= D_k^{1/\theta} && (6.9) \\ TD_k^{'} &= D_k^{'1/\theta} && (6.10) \\ TD_{kx} &= D_{kx}^{'1/\theta}, \forall x \in S_k && (6.11) \end{aligned}$$

$$TK_k = (TD_k, TD_k^{'}, \forall x \in S_k : TD_{kx}) \tag{6.12}$$

Finally, EV_k sends TK_k with the pseudonym PS_k to the ISO for auditing.

Evaluation Challenge Generation

The AGG generates the evaluation challenge *chlg* in the same way as that in PMQC, which is detailedly described in Subsection 4.2.2.

$$\begin{aligned} &CT = [C = M_2 \tilde{e}^s, C^{'} = g^s, (C_1 = f^{\varphi_1} q_{\rho(1)}^{-r_1}, C_1^{'} = g^{r_1}), \\ &\cdots, (C_l = f^{\varphi_l} q_{\rho(l)}^{-r_l}, C_l^{'} = g^{r_l}), \mathbf{L}, \rho()] \end{aligned} \tag{6.13}$$

$$chlg = (M_1, CT, TS, Sig_{AGG}\{H_3(M_1 \parallel CT \parallel TS)\}) \tag{6.14}$$

Different from that in PMQC, the AGG does not directly send the challenge *chlg* to EV_k. Instead, it sends the challenge *chlg* with the pseudonym PS_k to the ISO for auditing.

6.2.3 Charging Request Auditing

Based on the temperate key TK_k from EV_k and the evaluation challenge *chlg* from the AGG, the ISO audits EV_k's charging service request under pseudonym PS_k by pre-decrypting the CP-ABE ciphertext in the evaluation challenge *chlg* with the temperate key TK_k.

After receiving the evaluation challenge *chlg* from the AGG, the ISO checks *chlg*'s integrity by verifying the signature $Sig_{AGG}\{H_3(M_1 \parallel CT \parallel TS)\}$ inside of *chlg*. Then the ISO audits EV_k's charging service request based on the assessment on the resource condition of the AGG.

- If the ISO allows the AGG to accept more EVs for QGS, it pre-decrypts the CP-ABE ciphertext CT in *chlg* with EV_k's temperate key TK_k.

  Specifically, the ISO computes the subset $J_k \subseteq J$ satisfying

  $$\{\rho(j) : j \in J_k\} \subseteq S_k \tag{6.15}$$

  where J is the set of row index of the LSSS matrix $\mathbf{L}$ in CP-ABE ciphertext CT and j indicates the index of jth row in matrix $\mathbf{L}$.

  If the attribute set S_k in the EV_k's temperate key TK_k matches the access structure $\mathbb{A}$ described in matrix $\mathbf{L}$, there would be a set of constant $\{\omega_j \in \mathbb{Z}_p^* : j \in J_k\}$ satisfying

  $$\sum_{j \in J_k} \omega_j \cdot \mathbf{l}_j = (1, 0, \cdots, 0) \tag{6.16}$$

  Specifically,

  $$\sum_{j \in J_k} \omega_j \cdot \varphi_j = \sum_{j \in J_k} \omega_j \cdot \mathbf{l}_j \cdot \mathbf{y} = (\sum_{j \in J_k} \omega_j \cdot \mathbf{l}_j) \cdot \mathbf{y} = s \tag{6.17}$$

  Then the ISO can pre-decrypt the CP-ABE ciphertext CT and get the pre-decryption result $\{C, T\hat{C}\}$.

$$
\begin{aligned}
T\hat{C} &= \frac{e(C', TD_k)}{\prod_{j \in J_k}[e(C_j, TD'_k) \cdot e(C'_j, TD_{k\rho(j)})]^{\omega_j}} \\
&= \frac{e(g,g)^{\alpha s/\theta} \cdot e(g,g)^{s\beta t_k/\theta}}{\prod_{j \in J_k} e(g,g)^{\beta \varphi_j \omega_j t_k/\theta}} \\
&= \frac{e(g,g)^{\alpha s/\theta} \cdot e(g,g)^{s\beta t_k/\theta}}{e(g,g)^{(\beta t_k \sum_{j \in J_k} \varphi_j \omega_j)/\theta}} \\
&= \frac{e(g,g)^{\alpha s/\theta} \cdot e(g,g)^{s\beta t_k/\theta}}{e(g,g)^{s\beta t_k/\theta}} \\
&= e(g,g)^{\alpha s/\theta}
\end{aligned}
\tag{6.18}
$$

After successfully pre-decrypting the CP-ABE ciphertext, the ISO sends EV_k the permission $pmsn$ including the pre-decryption result $\{C, T\hat{C}\}$ and the plaintext $M1$.

$$
pmsn = \{M_1, C, T\hat{C}, TS, Sig_{ISO}[H_3(M_1 \parallel C \parallel T\hat{C} \parallel TS)]\} \tag{6.19}
$$

- If the ISO prohibits the AGG to accept more EVs for QGS, or if the attribute set S_k in the EV_k's temperate key TK_k mismatches the access structure $\mathbb{A}$ in matrix $\mathbf{L}$, the ISO sends EV_k the permission $pmsn$, which only includes the plaintext M_1.

$$
pmsn = \{M_1, TS, Sig_{ISO}[H_3(M_1 \parallel TS)]\} \tag{6.20}
$$

6.2.4 Service Eligibility Authentication

After the charging request auditing, EV_k responses to the AGG and authenticates itself with the group signature [49] on the messages M_1 and M_2 in $chlg$. If the group signature can be verified by AGG, EV_k is eligible to have charging service from the AGG.

Authentication Answering

When EV_k receives the permission $pmsn$ from the ISO, it first verifies the signature $Sig_{ISO}[H_3(M_1 \parallel TS)]$ inside $pmsn$ to check the integrity of the received permission $pmsn$.

- If $pmsn = \{M_1, C, T\hat{C}, TS, Sig_{ISO}[H_3(M_1 \parallel C \parallel T\hat{C} \parallel TS)]\}$, it indicates that the EV_k passes the AGG's evaluation and the ISO's auditing. If EV_k's service eligibility can be authenticated by the AGG, it can have QGS from the AGG.

  To pass the AGG's evaluation, EV_k first decrypts the pre-decryption result $\{C, T\hat{C}\}$ in order to get the message M_2.

  $$M_2 = \frac{C}{T\hat{C}^{\theta}} = \frac{M_2 e(g,g)^{s\alpha}}{[e(g,g)^{s\alpha/\theta}]^{\theta}} \tag{6.21}$$

  Then EV_k generates the group signature σ based on both M_1 and M_2, and sends it to the AGG. The detail of the group signature generation is formulated in Subsection 4.2.3.

- If $pmsn = \{M_1, TS, Sig_{ISO}[H_3(M_1 \parallel TS)]\}$, it indicates that the EV_k cannot have QGS from the AGG. The reason for the rejection may be the EV_k's attributes mismatching the AGG's access policy $\mathbb{A}$ or the ISO's limitation on total number of QGS EVs in the AGG. In such scenario, EV_k sends the AGG the group signature σ based on only M_1. The group signature is also generated in the same as that in Subsection 4.2.3.

After generating the group signature σ with the group signature private key GSK_k in the private key SK_k, EV_k sends it to the EVA for verification.

Answer Verifying

The EVA verifies the group signature σ from EV_k with the group signature public key GPK in the public key PK. If the group signature based on both M_1 and M_2 is verified, EV_k can have QGS. If the group signature based on M_1 is verified, EV_k can have BES. If the group signature verification is failed, the AGG rejects EV_k's charging service request. The detail for the group signature verification is formulated in Subsection 4.2.3.

6.2.5 Battery Monitoring

The battery monitoring phase in ePMQC is performed in the same way as that in PMQC. The detailed description for battery monitoring is in Subsection 4.2.4.

6.2.6 Bill Generation

The bill generation phase of ePMQC is same as that in PMQC shown in Subsection 4.2.5.

6.2.7 Revocation

The revocation phase of ePMQC is same as that in PMQC shown in Subsection 4.2.6.

6.3 Performance Enhancement

While achieving all the security features and security requirements of PMQC, the performance of ePMQC is significantly enhanced compared with PMQC. By introducing the ISO to pre-decrypt the CP-ABE ciphertext, the EV's computation overhead and storage overhead in CP-ABE decryption is dramatically reduced in ePMQC. This is a very attractive advantage for the EVs, which usually have very limited computation capability and storage capacity.

6.3.1 The EV's Computation Overhead

To further investigate the performance enhancement in computation overhead, ePMQC is compared with PMQC in terms of the EV's computation overhead in CP-ABE ciphertext decryption. Same as the assumption in Subsection 5.2.2, only the complex pairing operation, exponentiation operation in $\mathbb{G}$ and exponentiation operation in $\mathbb{G}_T$ are considered in the computation overhead evaluation. Let T_P be the time for a pairing operation, T_e be the time for an exponentiation operation in $\mathbb{G}$, and T_{eT} be the time for an exponentiation

operation in $\mathbb{G}_T$. The number of attributes satisfying $\{\rho(j) : j \in J_k\} \subseteq S_k$ is defined as N_{attr}.

Table 6.1: Notations in the Computation Overhead Evaluation of ePMQC

Symbols	Meanings
T_P	Time for a pairing operation
T_e	Time for an exponentiation operation in $\mathbb{G}$
T_{eT}	Time for an exponentiation operation in $\mathbb{G}_T$
N_{attr}	Number of attributes satisfying $\{\rho(j) : j \in J_k\} \subseteq S_k$

In PMQC, the EV's computation overhead is linear with the number of attributes N_{attr}. By analyzing the decryption steps for the CP-ABE ciphertext in Subsection 4.2.3, the EV's computation overhead is $T_P + (2T_P + T_{eT}) * N_{attr}$. In contrast, the EV's computation overhead in ePMQC is independent of the number of attributes N_{attr}. Instead of being linear with N_{attr}, the EV's computation overhead on CP-ABE ciphertext decryption in ePMQC remains to be the constant T_{eT} all the time. To further demonstrate the reduction of the EV's computation overhead, simulations are conducted under the same condition as that in Subsection 5.2.2. The results are shown in Figure 6.3.

6.3.2 The EV's Storage Overhead

In PMQC, the EV needs to store its private key SK_k, the AGG's public key pub_{AGG}, the challenge $chlg$ from the AGG and the generated group signature σ. In ePMQC, the EV's private key SK_k, the AGG's public key pub_{AGG}, the ISO's public key pub_{ISO}, the permission $pmsn$ from the ISO and the generated group signature σ are stored in the EV. Comparing the EV's stored items in each scheme shown in Table 6.2, only the unique items in each scheme are investigated.

According to the definitions of $chlg$ and $pmsn$ in Equation 4.23 and Equation 6.19, the EV's storage overhead in PMQC and ePMQC are shown in Table 6.3.

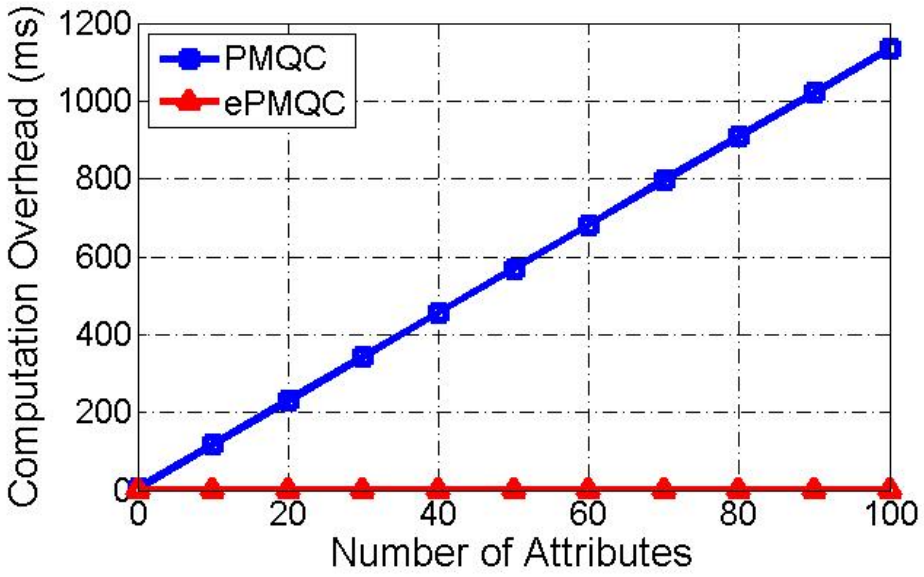

Figure 6.3: Comparison of the EV's Computation Overhead on Decryption

Table 6.2: Items Stored in the EV

Scheme	Items	Unique Items
PMQC	SK_k, pub_{AGG}, $chlg$, σ	$chlg$
ePMQC	SK_k, pub_{AGG}, pub_{ISO}, $pmsn$, σ	pub_{ISO}, $pmsn$

Based on the comparison in Table 6.3, further analysis is performed on the unique storage overhead in each scheme. l and n are the number of rows and the number of columns in the LSSS Matrix $\mathbf{L}$. $|\mathbb{Z}_p^*|$ is the size of a number in $\mathbb{Z}_p^*$, which is a multiplicative integer group under multiplication modulo p. $|\mathbb{G}|$ is the size of one element in multiplicative cyclic groups $\mathbb{G}$. $|\mathbb{G}_T|$ is the size of one element in multiplicative cyclic groups $\mathbb{G}_T$.

The detail of the storage overhead in PQMC and ePMQC are shown below:

- **PMQC:**

$$|CT| = (2l + 1) * |\mathbb{G}| + |\mathbb{G}_T| + l * n * |\mathbb{Z}_p^*| \tag{6.22}$$

Table 6.3: Comparison of the EV's Storage Overhead

Scheme	Storage Overhead	Unique Overhead
PMQC	$\|M_1\| + \|CT\| + \|TS\| + \|Sig_{AGG}\|$	$\|CT\|$
ePMQC	$\|M_1\| + \|C\| + \| + \|T\hat{C}\| + \|TS\| + \|Sig_{ISO}\| + \|pub_{ISO}\|$	$\|C\|$, $\|T\hat{C}\|$,$\|pub_{ISO}\|$

- **ePMQC:**

$$|C| + |T\hat{C}| + |pub_{ISO}| = 2 * |\mathbb{G}_T| + |pub_{ISO}| \tag{6.23}$$

Table 6.4: Notations in the Storage Overhead Evaluation of ePMQC

Symbols	Meanings
$\|\mathbb{Z}_p^*\|$	The size of a number in $\mathbb{Z}_p^*$
$\|\mathbb{G}\|$	The size of an element in group $\mathbb{G}$
$\|\mathbb{G}_T\|$	The size of an element in group $\mathbb{G}_T$
l	The number of rows in the LSSS Matrix $\mathbf{L}$
n	The number of columns in the LSSS Matrix $\mathbf{L}$

Specifically, the simulations on the EV's storage overhead are preformed under the group element size definition in Miracl Crypto Sdk [59]. $|\mathbb{Z}_p^*|$ is 1024 bits, $|\mathbb{G}|$ is 160 bits, $|\mathbb{G}_T|$ is 960 bits. The public key pub_{ISO} is a RSA public key with a length of 1024 bits. Based on the conditions declared above, simulation results are shown in Figure 6.4 and Figure 6.5. While the EV's storage overhead in PMQC going up with the increase in rows number and columns number of LSSS Matrix $\mathbf{L}$, the EV's storage overhead in ePMQC remains to be constant.

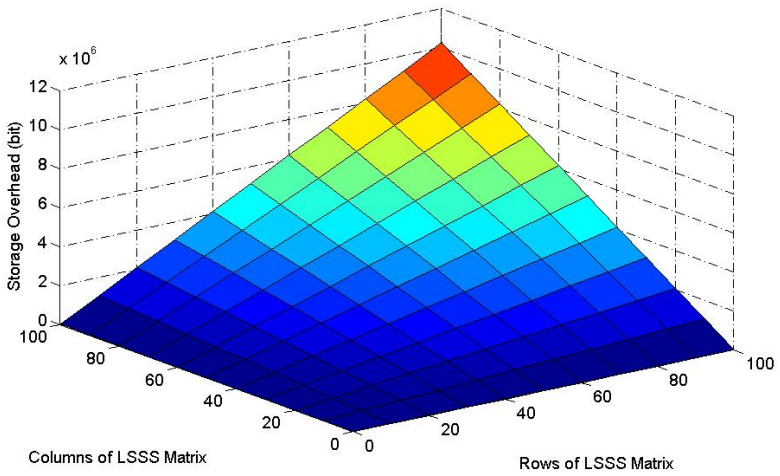

Figure 6.4: The EV's Storage Overhead in PMQC

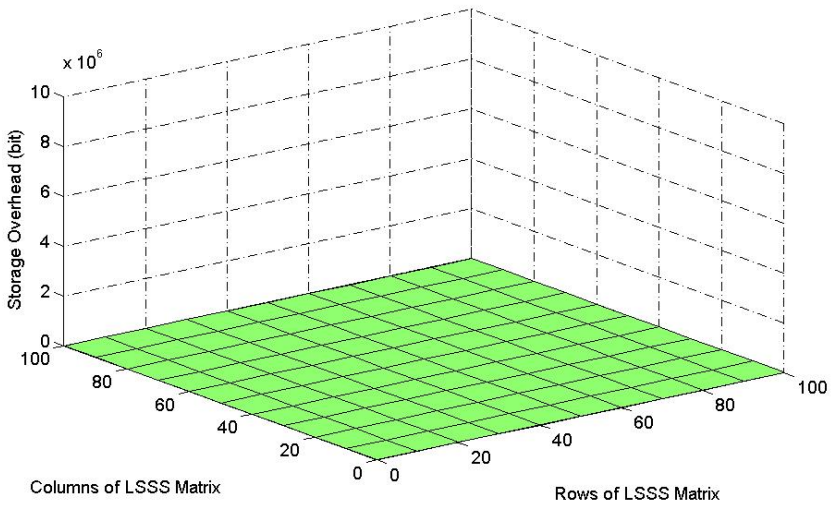

Figure 6.5: The EV's Storage Overhead in ePMQC

Chapter 7

Conclusion and Future Work

Recently, vehicle-to-grid (V2G) network attracts more and more attentions from both industries and academias due to its considerable environmental merits and economical benefits. However, the privacy-preservation concern is a major obstacle which makes people reluctant to join in the V2G network. In addition, the charging service with single service quality can hardly meet the market demand on diverse levels of charging services. In this thesis, a privacy-preserving multi-quality charging (PMQC) scheme for V2G network is proposed to offer the electric vehicle (EV) quality-guaranteed service (QGS) or best effort service (BES) without violating its privacy. Specifically, PMQC protects the EV's privacy, such as real identity, attributes, location and lifestyle, through identity-hidden authentication, attribute-hidden evaluation and anonymous bill generation. Security analysis demonstrates that the PMQC achieves the security requirements on privacy-preservation, fine-grained access control, traceability and secure revocation. Performance evaluation shows that PMQC can authenticate the EV with lower computation overhead compared with other schemes in V2G network. Based on PMQC, the extended privacy-preserving multi-quality charging (ePMQC) scheme can maintain the overall stability of V2G network and capacity of the regulation service provided by V2G network, by introducing the Independent System Organization (ISO) to audit the EV's charging service request. While satisfying all the security features and security requirements of PMQC, ePMQC achieves a significant reduction in the EV's computation overhead and storage overhead. In the

future, the following two aspects are expected to be explored:

- Both PMQC and ePMQC in this thesis focus on the privacy preserving issues. The security model is based on the assumption that all entities are honest but curious. In the future, privacy-preservation concerns under weaker security assumptions should be considered.
- The revocations in the proposed schemes only involve the EV's charging service eligibility. In the future, the efficient method to simultaneously revoke the EV's eligibility and attributes should be explored.

References

[1] H. Farhangi, "The path of the smart grid," *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18–28, 2010.

[2] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *PKC*, 2011, pp. 53–70.

[3] "NIST framework and roadmap for smart grid interoperability standards release 2.0," U.S.NIST, Tech. Rep., 2012.

[4] "The smart grid: An introduction," U.S. Department of Energy, Tech. Rep.

[5] "Interim report on the august 14, 2003 blackout," New York Independent System Operator, Tech. Rep., 2004.

[6] JakartaPost, "Massive blackout hits java, bali," http://www.thejakartapost.com/news/2005/08/19/massive-blackout-hits-java-bali.html, August 2005.

[7] NBCNews, "Lights flicker on after blackout in brazil," http://www.nbcnews.com/id/33844757/ns/world_news-americas/UuQY3VAo7IU, November 2009.

[8] NDTV, "Blackout for 19 states, more than 600 million indians," http://www.ndtv.com/article/india/blackout-for-19-states-more-than-600-million-indians-249537, July 2012.

[9] S. Amin and B. Wollenberg, "Toward a smart grid: power delivery for the 21st century," *IEEE Power and Energy Magazine*, vol. 3, no. 5, pp. 34–41, 2005.

[10] "Canada's emissions trends," Environment Canada, Tech. Rep., 2013.

[11] "National inventory report, 1990-2010: Greenhouse gas sources and sinks in canada," Environment Canada, Tech. Rep., 2012.

[12] "Backgrounder: Key features of canada's passenger automobile and light truck greenhouse gas emission regulations," Natural.Resources.Canada, Tech. Rep., 2011.

[13] C. Guille and G. Gross, "A conceptual framework for the vehicle-to-grid(V2G) implementation," *Energy Policy*, vol. 37, no. 11, pp. 4379–4390, 2009.

[14] H. Liang, B. J. Choi, W. Zhuang, and X. Shen, "Towards optimal energy store-carry-and-deliver for PHEVs via V2G system," in *IEEE INFOCOM*, 2012, pp. 1674–1682.

[15] A. Faruqui, R. Hledik, S. Newell, and H. Pfeifenberger, "The power of 5 percent," *The Electricity Journal*, vol. 20, no. 8, pp. 68–77, 2007.

[16] B. J. Kirby, *Frequency regulation basics and trends*. U.S. Department of Energy, 2005.

[17] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, Sept 2012.

[18] H. Khurana, M. Hadley, N. Lu, and D. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, no. 1, pp. 81–85, Jan 2010.

[19] A. Boulanger, A. Chu, S. Maxx, and D. Waltz, "Vehicle electrification: Status and issues," *Proceedings of the IEEE*, vol. 99, no. 6, pp. 1116–1138, June 2011.

[20] K. Shuaib, L. Zhang, and M. Gaouda, Ahmed andAbdel-Hafez, "A PEV charging service model for smart grids," *Energies*, vol. 5, pp. 4665–4682, 2012.

[21] A. Masoum, S. Deilami, P. Moses, and A. Abu-Siada, "Impacts of battery charging rates of plug-in electric vehicle on smart grid distribution systems," in *ISGT Europe*, 2010, pp. 1–6.

[22] Z. Yang, S. Yu, W. Lou, and C. Liu, "P2: Privacy-preserving communication and precise reward architecture for V2G networks in smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 697–706, 2011.

[23] X. Chen, F. Zhang, and S. Liu, "ID-based restrictive partially blind signatures and applications," *Journal of Systems and Software*, vol. 80, no. 2, pp. 164–171, 2007.

[24] H. Tseng, "A secure and privacy-preserving communication protocol for V2G networks," in *IEEE WCNC*, 2012, pp. 2706–2711.

[25] H. Liu, H. Ning, Y. Zhang, and L. Yang, "Aggregated-proofs based privacy-preserving authentication for V2G networks in the smart grid," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1722–1733, 2012.

[26] H. Tseng, "A robust aggregated message authentication protocol for vehicle-to-grid networks," in *19th ITS World Congress*, 2012.

[27] H. Liu, H. Ning, Y. Zhang, and M. Guizani, "Battery status-aware authentication scheme for V2G networks in smart grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 99–110, March 2013.

[28] H. Guo, Y. Wu, F. Bao, H. Chen, and M. Ma, "UBAPV2G: A unique batch authentication protocol for vehicle-to-grid communications," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 707–714, 2011.

[29] B. Vaidya, D. Makrakis, and H. Mouftah, "Security mechanism for multi-domain vehicle-to-grid infrastructure," in *IEEE GLOBECOM*, 2011, pp. 1–5.

[30] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, "UDP: Usage-based dynamic pricing with privacy preservation for smart grid," *Smart Grid, IEEE Transactions on*, vol. 4, no. 1, pp. 141–150, March 2013.

[31] M. Wen, R. Lu, K. Zhang, J. Lei, X. Liang, and X. Shen, "PaRQ: A privacy-preserving range query scheme over encrypted metering data for smart grid," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 1, pp. 178–191, June 2013.

[32] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient merkle-tree-based authentication scheme for smart grid," *IEEE Systems Journal*, vol. PP, no. 99, pp. 1–9, 2013.

[33] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, Nov 1976.

[34] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *EUROCRYPT*, 2005, pp. 457–473.

[35] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, 2006, pp. 89–98.

[36] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, 2007, pp. 195–203.

[37] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy*, 2007, pp. 321–334.

[38] D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical identity based encryption with constant size ciphertext," in *EUROCRYPT*, 2005, pp. 440–456.

[39] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, 2007, pp. 456–465.

[40] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in *Automata, Languages and Programming*, 2008, vol. 5126, pp. 579–591.

[41] D. Chaum and E. Van Heyst, "Group signatures," in *EUROCRYPT*, 1991, pp. 257–265.

[42] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A practical and provably secure coalition-resistant group signature scheme," in *CRYPTO*, 2000, pp. 255–270.

[43] G. Ateniese and G. Tsudik, "Some open issues and new directions in group signatures," in *Financial Cryptography*, 1999, pp. 196–211.

[44] L. Chen and T. P. Pedersen, "New group signature schemes," in *EUROCRYPT*, 1995, pp. 171–181.

[45] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," in *CRYPTO*, 1997, pp. 410–424.

[46] E. Bresson and J. Stern, "Efficient revocation in group signatures," in *PKC*, 2001, pp. 190–206.

[47] J. Camenisch and A. Lysyanskaya, "Dynamic accumulators and application to efficient revocation of anonymous credentials," in *CRYPTO*, 2002, pp. 61–76.

[48] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in *Proceedings of the 11th ACM Conference on Computer and Communications Security*, 2004, pp. 168–177.

[49] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *CRYPTO*, 2004, pp. 41–55.

[50] X. Boyen and B. Waters, "Compact group signatures without random oracles," in *EUROCRYPT*, 2006, pp. 427–444.

[51] M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions," in *Eurocrypt*, 2003, pp. 614–629.

[52] X. Boyen and B. Waters, "Full-domain subgroup hiding and constant-size group signatures," in *PKC*, 2007, pp. 1–15.

[53] E. Sortomme and M. El-Sharkawi, "Optimal charging strategies for unidirectional vehicle-to-grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 1, pp. 131–138, 2011.

[54] B. K. Sovacool and R. F. Hirsh, "Beyond batteries: An examination of the benefits and barriers to plug-in hybrid electric vehicles (PHEVs) and a vehicle-to-grid (V2G) transition," *Energy Policy*, vol. 37, no. 3, pp. 1095 – 1103, 2009.

[55] A. Brooks, E. Lu, D. Reicher, C. Spirakis, and B. Weihl, "Demand dispatch," *IEEE Power and Energy Magazine*, vol. 8, no. 3, pp. 20–29, 2010.

[56] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *CRYPTO*, 2001, pp. 213–229.

[57] Z. Yang, W. Lang, and Y. Tan, "A new fair micropayment system based on hash chain," in *IEEE International Conference on e-Technology, e-Commerce and e-Service*, 2004, pp. 139–145.

[58] W. Dai, "Crypto++ 5.6.0 benchmarks," Website at http://www.cryptpp.com/benchmarks.html, 2009.

[59] "MIRACL crypto SDK," Website at http://www.certivox.com/miracl/.