An Anonymous Payment System to Protect the Privacy of Electric Vehicles

Tianyu Zhao*, Chang Chen*, Lingbo Wei†, Mengke Yu*
*Key Laboratory of Electromagnetic Space Information, Chinese Academy of Sciences
Department of Electronic Engineering and Information Science
University of Science and Technology of China
†Department of Computer Science and Engineering
Shanghai Jiaotong University

***Abstract*—Electric vehicle is the automobile that powered by electrical energy stored in batteries. Due to the frequent recharging, vehicles need to be connected to the recharging infrastructure while they are parked. This may disclose drivers' privacy, such as their location that drivers may want to keep secret. In this paper, we propose a scheme to enhance the privacy of the drivers using anonymous credential technique and Trusted Platform Module(TPM). We use anonymous credential technique to achieve the anonymity of vehicles such that drivers can anonymously and unlinkably recharge their vehicles. We add some attributes to the credential such as the type of the battery in the vehicle in case that the prices of different batteries are different. We use TPM to omit a blacklist such that the company that offer the recharging service(Energy Provider Company, EPC) does not need to conduct a double spending detection.**

I. Introduction

Electric vehicle(EV) is futuristic and promising for its eco-friendly. As the world is suffering from the pollution of climate active gases and automobile exhaust is a major one, researchers are trying to find new energy to replace petroleum which is the primary resource now. EV is promising for it has a higher energy efficiency than vehicles that powered by combustion engine and EV dose not produce any exhaust emissions, thus EV can have a significant positive effect on environment.

However, EVs are also suffering from many deficiencies and limitations before their widespread adoption. Due to the fact that the battery used now can not last a long time before recharged, vehicles should be charged very frequently. Thus leads the problem we concern in this paper: the privacy of EVs(or drivers). Due to the need to recharge the batteries frequently, drivers' many private information, such as location privacy, may be disclosed according to the places and the time the EVs are charged. The disclosed privacy information includes the driver's home and company address, the time the driver at home and the time driver at work, the state of health of the driver and so forth. For example, if an EV is charged at two places every day, it is reasonable for us to deduce that the two places are driver's home and company addresses. If the EV is charged at or near a hospital or a rehabilitation centre, we can infer that the driver's health condition is not very good. If the vehicle is connected to the charging infrastructure at or near the driver's home, we can infer that the driver is at home and if the vehicle is disconnected from the charging infrastructure around home we can infer that the driver is leaving home. Some malicious adversaries can use these information to do something like home sales which bothers almost everyone when drivers at home. Some criminal may happen by using these information such as trace the driver to rob or conduct physical attacks. The malicious adversaries can also use the information to complete a burglary when the driver is not at home.

This work was supported in part by the Natural Science Foundation of China (NSFC) under Grants 61202140 and 61328208, by the Program for New Century Excellent Talents in University under Grant NCET-13-0548, by the Innovation

Vehicles powered by gasoline or natural gas do not have this problem because the vehicles may only be re-filled with gasoline once a week or longer, and the drivers prefers to pay cash instead of any other fashions of money. However, for EVs, although paying cash is totally anonymous since the cash is anonymous if we assume that the equipments of the charging network can not recognise the vehicle by any fashion, it is not convenient because the long charging time and frequent charging. Driver may choose to use credit card to pay the fee, this solution can not prevent the privacy from being violated either for the credit card is not anonymous and it is not safe to use the credit card frequently. Drivers can use a pre-paid card which is anonymous. However, if the card is not a one-time card, the linkability can also break the driver's privacy. We can use some cryptographic scheme to solve this problem and E-cash[1], [2] seems to be a promising one. However, drivers should withdraw and spend the coin that is a very small value one by one, which is very impractical. Although [3] proposes a scheme that can withdraw 2^l coins at one time, user has to spend them one by one. This makes the e-cash be used at the scenario that only need small amount of money. The way e-cash preventing the coins from double spending makes it not very effective, users can spend the same coin many times before being catched. And also, drivers may want a dedicated account for their charging process, it is not convenient to withdraw electric coins from bank to pay for their charging fee.

A. Contribution

Since existing payment systems can not support the s-cenario we describe above, we propose a scheme in this paper to protect drivers' privacy using anonymous credential technique and Trusted Platform Module(TPM). Using this scheme, drivers can anonymously yet unlinkably to charge their EVs and update the credentials after or before charging. We use anonymous credential technique to protect the privacy of drivers and the interests of EPC can also be protected by the authentication of the anonymous credentials. We also add some attributes to the anonymous credential to satisfy the diversity of the price. We use TPM to prevent users from cheating EPC, thus we can omit a blacklist to prevent a replay attack and omit a anonymity revocation mechanism because we assume that TPM will not do things that are illegal.

B. Construction

We will introduce some related work in section II, and then introduce some preliminaries in section III. In section IV, we describe the architecture of our scheme and the detail of scheme will be described in section V. After that, we analyze the security of our scheme in section VI. Finally we give a conclusion in section VII.

II. Related work

There are many literatures that using cryptographic schemes to protect the privacy of drivers. In [4], Li proposes a scheme using e-cash technique to implement an anonymous payment mechanism for EVs. The system has the shortcomings we discussed above and does not support the diversity of the prices. [5] proposes a scheme to search a charging station without disclosing the private information of the vehicle using blind signature technique in vehicular ad hoc network. However, the system in [5] does not put forward a payment mechanism.

Group signature scheme is used in [6] to protect the location privacy of vehicle. In [6], charging stations are the members of the group and malicious attackers can not recognize the identity of the charging station where the vehicles are re-filled. However, how to pay the fee is not described in [6].

In [7] and the follow-up work [8], they propose a scheme that can protect the location privacy of drivers and can also prevent the vehicles from being stolen and their system supports the Vehicle-to-Grid too. In [9], [10], Höfer proposes a complete framework for the charging of electric vehicle based on the modification of the ISO/IEC 15118 protocol and implement their work in [10] with a simulation environment.

However, all the schemes above has the same problem that they has to prepare a enormous blacklist to prevent customers from double spending such as in [7] and [8], a random number should be checked whether it is a used one and after that the identity should be put into the blacklist. They also do not support the diversity of prices of different attributes of EVs.

In our scheme, we use anonymous credential technique to balance the anonymity of drivers and the benefit of EPC and we also add some attributes to the anonymous credential to prove some properties of driver or EV. We use TPM to modify the scheme in [11] which inspires us to do this work and we assume that a TPM is totally trusted such that we do not concern the replay attack problem, so we omit a blacklist which will be very enormous if EVs are more and more. We also use the scheme in [12] to authenticate the TPM to make the charging station sure that it is indeed communicating with a TPM. We use the signature scheme in [13] which is based on Pairings to support the update of credential.

III. Preliminaries

A. Basic Assumptions

The following cryptographic assumptions are useful in our paper:

Assumption 1 (Strong RSA Assumption): Given a randomly chosen RSA modulus n and a random $z \in \mathbb{Z}_n^*$, it is hard to find $r > 1$ and $y \in \mathbb{Z}_n^*$ such that $y^r \equiv z \ (mod\ n)$.

Assumption 2 (Discrete Logarithm Assumption): Let $\mathbb{G}$ be a cyclic group of order n with generator g, given $h \in \mathbb{G}$, it is hard to compute $r \in \mathbb{Z}_n$ such that $h = g^r$.

B. Zero-Knowledge Proof

We use notations introduced by Camenisch and Stadler [14] for various proofs of knowledge of discrete logarithms. For instance,

$$PK\{(\alpha, \beta, \gamma) : y = g^\alpha h^\beta \wedge \tilde{y} = \tilde{g}^\alpha \tilde{h}^\gamma \wedge (u \leq \alpha \leq v)\}$$

denotes a *"zero-knowledge Proof of Knowledge of integers* α, β *and* γ *so that* $y = g^\alpha h^\beta$ *and* $\tilde{y} = \tilde{g}^\alpha \tilde{h}^\gamma$ *holds, where* $u \leq \alpha \leq v$*,"* where $y, g, h, \tilde{y}, \tilde{g}$ *and* $\tilde{h}$ are elements of some groups $\mathbb{G} = \langle g \rangle = \langle h \rangle$ *and* $\tilde{\mathbb{G}} = \langle \tilde{g} \rangle = \langle \tilde{h} \rangle$.The Greek letters denote the quantities that are being proved, while all other parameters can be known by the verifier.

C. Bilinear Maps

Let $\mathbb{G}$ and $\mathbb{G}_t$ be two groups of prime order p, and g is a generator of $\mathbb{G}$. We can define $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_t$ as a bilinear map between the $\mathbb{G}$ and $\mathbb{G}_t$. From the describing above, we can conclude that e should satisfies the following properties:

1) **Bilinear:** for all $x, y \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p$ we have $e(x^a, y^b) = e(x, y)^{ab}$.
2) **Non-degenerate:**$e(g, g) \neq 1$.
3) **Computable:** for any $x, y \in \mathbb{G}$, there should be an efficient algorithm to compute $e(x, y)$.

D. Camenisch-Lysyanskaya Signature Scheme

Camenisch and Lysyanskaya(C-L) proposed a signature scheme in [13] which can be described as follow:

Key Generation. Let $\mathbb{G}$ and $\mathbb{G}_t$ be two groups of order p and g is a generator of $\mathbb{G}$. $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_t$ is a bilinear map. If we have $l + 1$ messages to be signed, we randomly choose $x, y, z_1, \ldots, z_l \in \mathbb{Z}_p$. The private key is $sk = (x, y, \{z_i\})$ and the public key is $pk = (X, Y, \{Z_i\}, e, g, \mathbb{G}, \mathbb{G}_t, p)$ where $X = g^x, Y = g^y, Z_i = g^{z_i}$ for $i = 1, 2, ..., l$.

Signing. Supposing $(m_0, \ldots, m_l)$ are the messages to be signed, we can randomly choose $a \in \mathbb{G}$,and using sk,

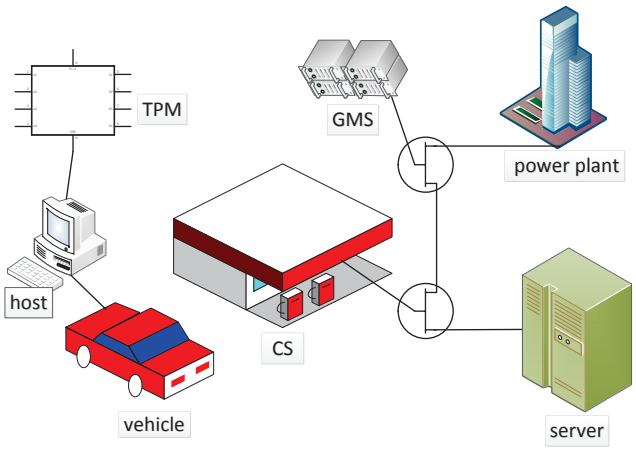

Fig. 1. Architecture of our system

pk to compute $A_i = a^{z_i}, b = a^y, B_i = A_i^y$ and $c = a^{x+xym_0} \prod_{i=1}^{l} A_i^{xym_i}$ for $i = 1, 2, \ldots, l$. The signature is

$$\sigma = (a, \{A_i\}, b, \{B_i\}, c).$$

Verification. Anyone that gets message$(m_0, \ldots, m_l)$ can use pk to verify signature $\sigma = (a, \{A_i\}, b, \{B_i\}, c)$ as follow:

1) $\{A_i\}$ are formed correct:$e(a, Z_i) = e(g, A_i)$.
2) b and $\{B_i\}$ are formed correct:$e(a, Y) = e(g, b)$ and $e(A_i, Y) = e(g, B_i)$.
3) c is formed correct:

$$e(X, a) \cdot e(X, b)^{m_0} \prod_{i=1}^{l} e(X, B_i)^{m_i} = e(g, c)$$

.

IV. Architecture

In this section we give an explanation on the features of our scheme. Fig. 1 gives an overview of different entities in our scheme and our system is composed of the following entities:

Energy Provider Company(EPC). EPC provides the vehicle with electric energy and it is composed of:

1) *Server*. Server can issue credentials to EVs and it interacts with EVs and GMS to confirm the price of electric energy and the bill to update the credentials of EVs. All the computation of EPC is done by server.
2) *Grid Manager Server(GMS)*. EPC uses GMS to manage electric energy. GMS connects power plant so it knows the current price considering different conditions. GMS also control whether the charging station charge the vehicles.
3) *Charging station(CS)*. CS connects with EVs, the GMS and server. CS has applications such as Register, Top-up, Charging, etc that are controlled by server and GMS. Charging station is like a valve controlled by GMS.

Vehicle. It is the consumer of our system, the equipments in the vehicle are as follow:

1) *Host*. A host refers to the computer in the EV that is being charged. Most of the computation of EV is done by host.
2) *TPM*. A TPM is a trusted platform module that is embedded in the host. It is a chip with limited computation and storage.

In our system, we not only protect the privacy of EVs, we also prevent EVs(drivers) from cheating the EPC by forging or replay the credential he got. We use anonymous credential technique to achieve this goal. A TPM is a chip that can be totally trusted, i.e. TPM will not do things illegal. Using TPM, we can omit a blacklist because TPM will not give the server a same identity twice. However, a TPM is just a chip that has limited computing power, so we hope the computation of EV can be done by host as much as possible.

A. Protocols of our system

In our scheme, EPC runs a *Setup* process to generate the keys needed in the system at first. After that, a TPM should register with EPC and this process can just be performed once for a TPM. Then driver should charge money into the credential and after all the process above, a driver can use the credential freely.

EPC Setup. In this process, EPC generates a key-pair (sk, pk) for the C-L signature scheme, publishes pk and stores sk.

EV Register. TPM sends the necessary information to the server of EPC to open an account and then server issues an anonymous credential to TPM and host.

EV Top-up. TPM and host first present their credential to server and carry an interactive protocol with the server. TPM and host obtain an updated anonymous credential with increased balance.

Charge. TPM and host present their credential and some attributes of the vehicle to the server. After that, server asks GMS the price of the current electric energy in the case of dynamic price. If the remain balance in the credential is larger than the require amount, GMS tells CS to start to charge the vehicle. After that, TPM and host get an updated credential with decremented balance.

B. Attributes of our system

We add some attributes to our credential system in the case of different prices of different situations. Different types of vehicles(batteries) may have different prices and we use t_v to denote the battery type of a EV. It is realistic to assume that there are many EPCs that offer the charging service, so we add a com attribute to the credential to indicate the EPC that the credential was issued by. If a driver wants to charge his EV at a foreign country, it is very possible he has to charge his EV at a different EPC. A EPC can offer a roaming service to customers from other companies.

However, the number of attribute is not fixed and we can also add some other attributes at any time to the credential system. Considering the scenario that a company can offer a special-charging service for the driver who live in a special

TABLE I
NOTATIONS USED IN OUR SYSTEM

$\mathbb{G}$, $\mathbb{G}_t$	Groups of order p
g	Generator of $\mathbb{G}$
e	A bilinear map : $\mathbb{G} \times \mathbb{G} \to \mathbb{G}_t$
sk	Private key of EPC
pk	Public key of EPC
t_v, com, con	The attributes of credential that can't be changed
id, s	The attributes of credential that can be updated
$h(\cdot)$	Hash function
$\|\|$	Concatenation function

block, we can add the information that where the driver live into the credential system. Other preferential services can also add attributes to our credentials system, we use con to denote them.

C. Communication

We can infer from section IV-A that CS is just a front-end terminal which is like a relay, so we omit it when we describe the communication between vehicles and server.

In our scheme, it is unrealistic to assume that TPM and server can communicate with each other directly and most communication of a TPM is controlled by host. In consideration of TPM's work that doing some computation about id and attributes is not very much, TPM can encrypt all the work using server's public key(different form pk) thus host can not know id even though he gets the ciphertext. We can use a timestamp to prevent EV from conducting the replay attack. If all the communication is controlled by host, how dose a server can trust a message is indeed from a TPM? If we use TPM's private key to sign a message, then the property of unlinkability is broken. If all the TPMs use the same public-private key pair, then server can be sure that the message is from a TPM if the message is indeed from TPM. But if one TPM compromises, server will not recognize the real TPM from a fake one. A good solution is to use the technique in [12] and thus TPM can hide the identity of TPM and server can also authenticate the TPM.

V. SCHEME

We have mentioned before in our paper that a TPM is only a chip with limited computing power. So we prefer that the computation of the TPM can be outsourced to the host that TPM embedded in as much as possible.

We first list the notations used in our system in TABLE I

A. EPC Setup

EPC generates a key-pair (sk, pk) for the C-L signature scheme where

$$\begin{cases} sk = (x, y, z_1, z_2, z_3) \\ pk = (X, Y, Z_1, Z_2, Z_3, e, g, \mathbb{G}, \mathbb{G}_t, p) \end{cases}$$

sk and pk satisfy the requirement of C-L signature we mentioned at section III-D. Then EPC publishes pk and stores sk.

Details: Host and TPM choose parameters that are needed respectively and after some computation with server interactively, TPM and host get an anonymous credential σ:

1) Host randomly chooses $r_{id}, r_s \in \mathbb{Z}_p$ to hide id (host does not know id) and s (s=0) respectively. Then host computes $\hat{C}_{id} = Z_1^{r_{id}}$ and $C_s = Z_3^{r_s} (C_s = Z_3^{r_s} = Z_2^s Z_3^{r_s}$ when $s = 0)$. Host sends C_s to server and $\hat{C}_{id}$ to TPM.
2) TPM randomly chooses $id \in \mathbb{Z}_p$ and computes $C_{id} = g^{id} \hat{C}_{id}$ and sends C_{id} to server.
3) TPM and host together produce a signature of knowledge:
$$SPK\{(\alpha, \beta, \gamma) : C_{id} = g^\alpha h^\beta \wedge C_s = Z_3^\gamma\} \quad (1)$$
this can be done using a $\Sigma - protocol$ in Fig. 3
4) if equation (2) holds, server randomly chooses $k \in \mathbb{Z}_p$ and computes $a = g^k, b = a^y, A_i = a^{z_i}, B_i = A_i^y, c = a^x (C_{id} C_s)^{kxy}$ for $i = 1, 2, 3$. Then server sends the signature
$$\sigma = (a, \{A_i\}, b, \{B_i\}, c)$$
to host.
5) TPM computes $h(id||t_v)$, $h(id||com)$, $h(id||con)$ and sends them to host.

Fig. 2. EV Register

Detail: the $\Sigma - protocol$ works as follow:

1) host randomly chooses $r'_{id}, r_{r_{id}}, r_{r_s} \in \mathbb{Z}_p$, computes $\tilde{C}_{id} = g^{r'_{id}} Z_1^{r_{r_{id}}}$ and $\tilde{C}_s = Z_3^{r_{r_s}}$ and sends $(\tilde{C}_{id}, \tilde{C}_s)$ to server.
2) Server sends a random challenge c to TPM and host.
3) host computes $s_{r_{id}} = r_{r_{id}} + c \cdot r_{id}$, $s_{r_s} = r_{r_s} + c \cdot r_s$ and sends $(s_{r_{id}}, s_{r_s})$, r'_{id} to server and TPM respectively.
4) TPM computes $s_{id} = r'_{id} + c \cdot id$ and sends it to server.
5) Server checks whether
$$\begin{cases} g^{s_{id}} Z_1^{s_{r_{id}}} \stackrel{?}{=} \tilde{C}_{id} (C_{id})^c \\ Z_3^{s_{r_s}} \stackrel{?}{=} \tilde{C}_s (C_s)^c \end{cases} \quad (2)$$

Fig. 3. The detail of the $\Sigma - protocol$ of Fig 2

B. EV Register

Register can just be performed once for a TPM. TPM randomly chooses id and hides it from host. Other parameters can be chosen by host. TPM uses a hash function $h(\cdot)$ that using the attributes of the vehicle to prevent the host from changing the attributes, then host uses the results of the hash function as parts of the anonymous credential to selective disclose to the server. The protocols are as Fig. 2.

We can infer from Fig. 2 that,

$$\begin{aligned} c &= a^x (C_{id} C_s)^{kxy} \\ &= a^{x + xyid} A_1^{xyr_{id}} A_2^{xys} A_3^{xyr_s} \end{aligned} \quad (3)$$

Host can check the validity of σ and then host gets an anonymous credential on id with $s = 0$. So the anonymous credential is $(\sigma, h(id||t_v), h(id||com), h(id||con))$. We can infer that, attributes in σ can be updated and attributes in hash functions can not be changed. The attributes in hash functions can be selective disclosed by host to the server.

C. Top-up

To top a credential up, host and TPM should blind the credential first to make the signature anonymous and unlinkable. Then host and TPM send the blinded credential to server, they also sends d which denotes the amount of energy that the

Detail: The authentication phase can be carried out as follow:

1) Host randomly chooses $r_1, r_2 \in \mathbb{Z}_p$ and then turns the credential to $\sigma' = (a^{r_1}, \{A_i^{r_1}\}, b^{r_1}, \{B_i^{r_1}\}, c^{r_1 r_2})$ for $i = 1, 2, 3$. The blinded credential we donate as
$$\sigma' = (a', \{A_i'\}, b', \{B_i'\}, c')$$
2) Host computes $v_\sigma = e(g, c')$, $v_{r_{id}} = e(X, B_1')$, $v_s = e(X, B_2')$,$v_{r_s} = e(X, B_3')$, $v' = e(X, a')$ and $\hat{v} = e(X, b')$ then sends $\hat{v}$ to TPM.
3) TPM computes $\tilde{v} = \hat{v}^{id}$ and sends it to host.
4) host computes $v = e(X, a') \cdot \tilde{v}$.
5) Host sends (σ', d) to server. TPM sends id to server.
6) Server computes $v_\sigma = e(g, c')$, $v_{r_{id}} = e(X, B_1')$, $v_s = e(X, B_2')$,$v_{r_s} = e(X, B_3')$ and $v = e(X, a') \cdot e(X, b')^{id}$.
7) TPM and host together produce a signature of knowledge:
$$SPK\{(\alpha, \beta, \gamma, \delta) : v_\sigma^\alpha = v v_{r_{id}}^\beta v_s^\gamma v_{r_s}^\delta\}$$
using the same method in Fig.3

Fig. 4. Authentication Phase

consumer wants to buy to server. After that, host and TPM together prove to the server that the credential is correct. Then server will interact with host and TPM to update the credential. So we use *authentication* and *update* two phases to achieve the Top-up goal.

1) Authentication: After authentication, host and TPM prove the validity of the blinded anonymous credential and any mistake can make the authentication halt. We describe the detail of authentication in Fig.4

After the authentication phase, host and TPM prove to the server that they have a valid credential and then they update the credential together.

2) Update: After the authentication phase, server interact with host and TPM to update the credential, the detail of update is described in Fig.5

We can see that

$$\begin{aligned} c'' &= (\tilde{c}'')^{r_2^{-1}} \\ &= (c'(C_{id+id'} C_{s+|d|})^{xy})^{\tilde{r} r_2^{-1}} \\ &= (a^{x+xy(id+id')} A_1^{xy(r_{id}+r_{id'})} A_2^{xy(s+|d|)} A_3^{xy(r_s+1)})^{r_1 \tilde{r}} \end{aligned} \tag{4}$$

By comparing (4) with (3), we can note that host gets a new (updated) credential on $(id + id', r_{id} + r_{id'}, s + |d|, r_s + 1)$ with all the attributes updated to $\mathcal{H}(id+id'||attribute_i)$ where $attribute_i$ denotes t_v, com and con. Server does not know $id + id'$ and neither does host. So after the update, $id + id'$ is hidden from server to achieve the anonymity and unlinkability of our scheme. Host dose not know $id + id'$, so he can not cheat server when charging.

D. Charge

Charging is also a process of authentication and update and what on the contrary to the update phase of Top-up in our scheme is that we use $A_2'^{-|d|} A_3'$ to replace $A_2'^{|d|} A_3'$. So we should prove that $s > |d|$ which can be done easily using **Range Proof** [15] and we will not describe it in this paper. When conducting the authentication phase, host should selectively send the attributes that can not changed and their

Detail: The update phase can be carried out as follow:

1) Server computes $C'_{s+|d|} = (A_2')^{|d|} A_3'$ and then sends it to host.
2) TPM randomly chooses id' and computes $\hat{C}_{id+id'} = (a')^{id'}$, then TPM sends it to host.
3) Host randomly chooses $r_{id'}$, computes $C_{id+id'} = (\hat{C}_{id+id'}(A_1')^{r_{id'}})^{r_2}$ and $C_{s+|d|} = (C'_{s+|d|})^{r_2}$ after he checks the correctness of $C'_{s+|d|}$, then sends $(C_{id+id'}, C_{s+|d|})$ to server.
4) TPM and host together produce a signature of knowledge:
$$SPK\{(\alpha, \beta, \gamma, \delta, \epsilon, \zeta) : C_{id+id'} = (a')^\alpha (A_1')^\beta \wedge C'_{s+|d|} = (C_{s+|d|})^\gamma \wedge v_\sigma^\gamma = v v_{r_{id}}^\delta v_s^\epsilon v_{r_s}^\zeta\}$$
using the same method in Fig.3.
5) If the proof above hold, server randomly chooses $\tilde{r} \in Z_p$ and update the signature to
$$\tilde{\sigma}'' = (a'^{\tilde{r}}, \{A_i'^{\tilde{r}}\}, b'^{\tilde{r}}, \{B_i'^{\tilde{r}}\}, (c'(C_{id+id'} C_{s+|d|})^{xy})^{\tilde{r}})$$
which we denote as
$$\tilde{\sigma}'' = (a'', \{A_i''\}, b'', \{B_i''\}, \tilde{c}'')$$
Server sends $\tilde{\sigma}''$ to host.
6) Host computes $c'' = (\tilde{c}'')^{r_2^{-1}}$ to get a updated credential
$$\sigma'' = (a'', \{A_i''\}, b'', \{B_i''\}, c'')$$
7) TPM computes $h(id+id'||t_v)$, $h(id+id'||com)$, $h(id+id'||con)$ and sends them to host.

Fig. 5. Update Phase

values to server to get a privilege to charge the battery. Server can verify the attributes by checking whether the values, say $\hat{h}(id||attribute_i)$, equal to the the results that server computes, i.e.
$$h(id||attribute_i) = \hat{h}(id||attribute_i) \tag{5}$$

VI. Security Analysis

We assume that C-L signature [13] and DAA scheme [12] are secure. It will not lose anonymity and unlinkability for TPM to send id to server because server does not know the id choosen at the last update process.

For the attributes that can not be changed, we use a hash function which is one-way. Host does not know the latest id, so he can not deduce the result of $h(id||attributes)$ and even though he knows $h(attributes)$, he can not deduce id because of the one-way property of hash function. Every time a credential is updated, $h(attributes)$ are changed using the latest id that only TPM knows. Host can not change the attributes because he does not know id and he can not use it to carry out a replay attack either because (5) will not hold.

During EV Register phases, TPM and host send C_{id} and C_s which are the Pedersen Commitment [16] of id and s even though $s = 0$ to server and the Pedersen commitment is secure under the discrete logarithm assumption. After that, TPM and host use zero-knowledge proof to prove id, r_{id} and r_s, thus they do not disclose any useful information to server.

During authentication phase, TPM and host use r_1 and r_2 to blind the credential to satisfy the unlinkability property of our system. They use zero-knowledge proof to prove the correctness of the credential they hold, so they do not disclose any information to the server. And during the update phase,

TPM sends $\hat{C}_{id+id'} = (a')^{id'}$ to host. Under the discrete logarithm assumption, host can not know id'.

VII. Conclusion

In this paper we propose a scheme that can protect the privacy of electric vehicle(or the driver) using anonymous credential technique and TPM. Our scheme allows drivers to anonymously and unlinkably to use credentials to charge their vehicles . We add a Trusted Platform Module(TPM) to D. Slamanig's work[11] to solve the problem that needing a huge blacklist and omit the process of checking whether the current id is on the blacklist. In our scheme, we use a timestamp to prevent server from suffering from a replay attack. We also add some attributes to the credential, the attributes that can be changed are added to σ and the others that can not be changed are added into the hash functions to satisfy the selective disclose attribute of anonymous credential[17].

References

[1] D. Chaum, "Blind signatures for untraceable payments," in *Advances in cryptology*. Springer, 1983, pp. 199–203.

[2] D. L. Chaum, "Blind signature systems," Jul. 19 1988, uS Patent 4,759,063.

[3] J. Camenisch, S. Hohenberger, and A. Lysyanskaya, "Compact e-cash," in *Advances in Cryptology–EUROCRYPT 2005*. Springer, 2005, pp. 302–321.

[4] C. Li, "Anonymous payment mechanisms for electric car infrastructure," Ph.D. dissertation, Masters thesis, LU Leuven, Leuven, 2011.

[5] T. W. Chim, J. C. L. Cheung, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "Spcs: Secure and privacy-preserving charging-station searching using vanet," *Journal of Information Security*, vol. 3, p. 59, 2011.

[6] T. Frosch, S. Schäge, M. Goll, and T. Holz, "Improving location privacy for the electric vehicle masses."

[7] J. K. Liu, M. H. Au, W. Susilo, and J. Zhou, "Enhancing location privacy for electric vehicles (at the right time)," in *Computer Security–ESORICS 2012*. Springer, 2012, pp. 397–414.

[8] M. H. AU, J. K. LIU, J. FANG, Z. L. JIANG, W. SUSILO, and J. ZHOU, "A new payment system for enhancing location privacy of electric vehicles," *IEEE transactions on vehicular technology*, vol. 63, no. 1, pp. 3–18, 2014.

[9] Höfer, "privacy-preserving charging for emobility," Master's thesis, Distributed and Embedded Security Faculty of Electrical Engineering, Mathematics and Computer Science University of Twente The Netherlands, 2013.

[10] C. Höfer, J. Petit, R. Schmidt, and F. Kargl, "Popcorn: privacy-preserving charging for emobility," in *Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles*. ACM, 2013, pp. 37–48.

[11] D. Slamanig, "Efficient schemes for anonymous yet authorized and bounded use of cloud resources," in *Selected Areas in Cryptography*. Springer, 2012, pp. 73–91.

[12] E. Brickell, J. Camenisch, and L. Chen, "Direct anonymous attestation," in *Proceedings of the 11th ACM conference on Computer and communications security*. ACM, 2004, pp. 132–145.

[13] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," in *Advances in Cryptology–CRYPTO 2004*. Springer, 2004, pp. 56–72.

[14] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," in *Advances in CryptologyłCRYPTO'97*. Springer, 1997, pp. 410–424.

[15] W. Mao, "Guaranteed correct sharing of integer factorization with off-line shareholders," in *Public Key Cryptography*. Springer, 1998, pp. 60–71.

[16] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Advances in CryptologyłCRYPTO91*. Springer, 1992, pp. 129–140.

[17] T. Zhao, C. Chen, L. Wei, and M. Yu, "An anonymous payment system to protect the privacy of electric vehicles," in *2014 International Conference on Wireless Communications and Signal Processing (WCSP) (WCSP'14)*, Hefei, Anhui Province, P.R. China, Oct. 2014, pp. 845–850.