Secure Automated Valet Parking: A Privacy-Preserving Reservation Scheme for Autonomous Vehicles

Cheng Huang, *Student Member, IEEE*, Rongxing Lu, *Senior Member, IEEE*, Xiaodong Lin, *Fellow, IEEE*, and Xuemin Shen, *Fellow, IEEE*

***Abstract*—It is believed that automated valet parking (AVP) system has great potential to mitigate the parking headache for the future smart city, as it can provide on-demand parking services, bringing immense benefits from energy saving for vehicles to time saving for drivers. For an AVP system, parking reservation is an indispensable part so that vehicles can accomplish automated parking in accordance with the reserved parking information. However, the reservation requests may not only reveal the driver identity, but also disclose his/her sensitive locations, e.g., the most visited places, which are of great concerns to users. To deal with this challenge, the anonymous techniques can be naturally applied during parking reservation, but directly applying the anonymous techniques in AVP will introduce a new security issue, i.e., the anonymous user may maliciously crash the AVP system by repetitively sending the reservation requests, which is called "double-reservation attack." In this paper, we propose a new privacy-preserving reservation scheme for securing AVP system. Specifically, each anonymous user must have only one valid reservation token at any moment, and the token can only be used for booking one vacant parking space once. The proposed scheme does not only preserve the user's identity privacy and location privacy but also prevents the "double-reservation attack" based on several elegant building blocks, i.e., zero-knowledge proofs of knowledge and proxy resignature. Detailed security analysis confirms the security properties of our proposed scheme. In addition, extensive simulations are conducted to compare our proposed scheme with three previous schemes, and the experiment results demonstrate that our scheme is also much efficient in a WiFi-based testbed.**

***Index Terms*—Automated valet parking, anonymity, location privacy, parking reservation, autonomous vehicles.**

I. Introduction

PARKING, as one of the perennial headaches of urban life, is a common but especially vexing problem for big cities.

Manuscript received March 13, 2018; revised June 25, 2018; accepted August 18, 2018. Date of publication September 13, 2018; date of current version November 12, 2018. This work was supported by a research grant from The Intel Corporation, Inc. The review of this paper was coordinated by Dr. A.-C. Pang. *(Corresponding author: Cheng Huang.)*

C. Huang and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: c225huan@uwaterloo.ca; sshen@uwaterloo.ca).

R. Lu is with the Faculty of Computer Science, University of New Brunswick, Fredericton, NB E3B 5A3, Canada (e-mail: rlu1@unb.ca).

X. Lin is with the Department of Physics and Computer Science, Wilfrid Laurier University, Waterloo, ON N2L 3C5, Canada (e-mail: xlin@wlu.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2018.2870167

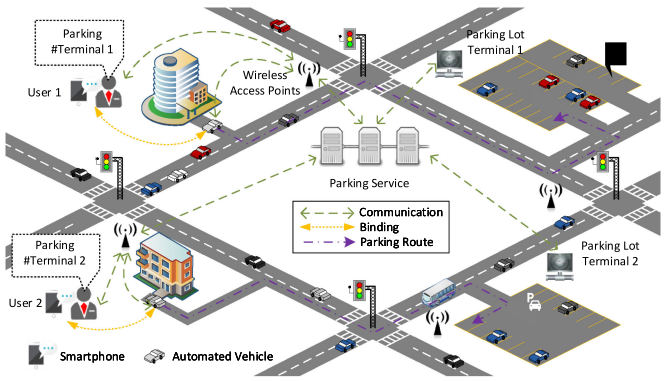


Fig. 1. An automated valet parking scenario where the user can make parking reservation remotely through the communication.

This hassle is not only caused by the fast-growing number of vehicles, but also by the unbalanced distribution of parking lots and the lack of a parking guidance system. Hence, a fantastic solution, automated valet parking (AVP) [1] has been proposed recently, which relies on the autonomous driving techniques to avoid the defects of valet parking. Taking the AVP solution of Daimler-Benz company as an example [2], an automated valet parking mission starts when a driver drops the AV in a designated drop-off area, and then he/she can monitor and control the autonomous vehicle (AV) via the smartphone until the parking task is accomplished. On one hand, the sensors installed in the parking lot can help steer the parking process; on the other hand, the AV itself can perform safe driving manoeuvres in response to the commands from the parking infrastructure and stop the vehicle if an emergency situation takes place.

Though the Daimler-Benz's AVP system has been licensed by the government, it is still an incomplete autonomous parking solution. It just achieves the "partial self-parking functionality" since the AV has to be dropped at a drop-off area but not anywhere else. Similarly, another automotive company, ZongMu Technology [3] has just released its self-parking products, and announced that its goal is to achieve a remote automated valet parking solution step by step using the close-to-market sensors. As shown in Fig. 1, when a driver has reached his/her destination (e.g., place of work, gym, or hospital), he/she can leave the vehicle and control the self-parking process by the smartphone remotely, e.g., following the parking route in a high-level parking scenario. Considering the low velocity of AV (up to

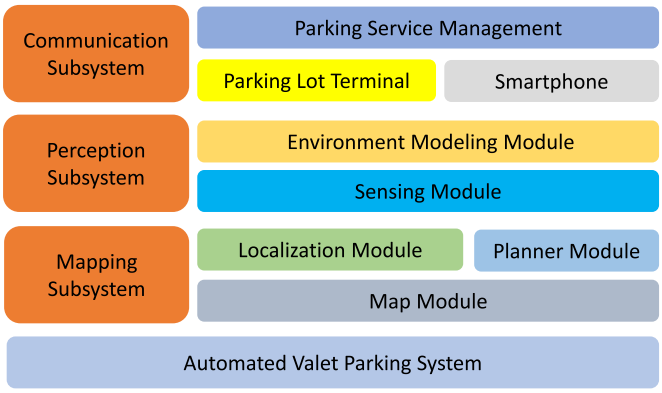


Fig. 2. The diagram of an AVP system.

30 km/h) and the light traffic situation, the deployment of AVP is mostly limited to the immediate vicinity of the location where the driver leaves the vehicle, which will reduce the requirements regarding the capabilities of AV significantly.

Generally, an AVP system can be virtualized as three subsystems [4]: mapping, perception, and communication as shown in Fig. 2. The mapping subsystem involves the localization module, the planner module, and the map module: the localization module supports GPS and GPS-denied localization to avoid collisions and plans appropriate motions; the planner module is responsible for generating an optimal trajectory from a start position to a destination, including on-road trajectory and the trajectory into the parking bay inside the parking lot; the map module creates a high-precision 3D geometric map which contains the detailed on-road and parking lot information. The perception subsystem consists of the sensing module and environment modeling module: the sensing module collects the sensing information from the LIDAR, radar and multiple cameras; the environment modeling module constructs a dynamic environment model based on the sensing information, such as detecting and tracking moving vehicles and pedestrians. The communication subsystem takes charge of sending/receiving the messages/commands to/from the parking service provider, the parking lot terminal and the driver's smartphone. The above modules are hot research topics for an AVP system, but less works have been done in the related area of security and privacy issues (see the references in Section VI).

Different from the traditional parking systems, the AVP system requires the driver to reserve a nearby vacant parking space in advance so that his/her vehicle can park itself autonomously without human intervention. However, this reservation procedure is under risk of privacy violation. In specific, when parking is required, the AVP system requires the AV to report its current location to the parking service provider (PSP) via the communication subsystem so that a better parking choice can be offered to locate an optimal nearby parking space for that vehicle. In this situation, the PSP will learn the personal and location-privacy-sensitive information, such as the most visited places of the vehicle, by investigating its uploaded locations [5], [6], which means that the driver's location privacy has been compromised. To address the privacy issue, a naive way is to introduce the anonymous mechanism into the AVP system: each autonomous vehicle will have plenty of pseudonyms which can also be authenticated by the PSP to protect the driver's privacy. Since the location privacy attacking method [7] needs at least four continuous location points in a trace, with both spatial relation and temporal relation, to identify a particular driver, the anonymous mechanism is effective due to the discrete characteristic of the parking behavior. In the parking scenario, the PSP cannot obtain four continuous location points from the AVP system because the average time interval between two parking demands is long enough.

From another perspective, the reserved parking space will be kept until the automated vehicle finishes the parking process or the reservation is expired, which gives the chance for malicious drivers to launch the "Double-Reservation Attack". The drivers cannot be assumed to behave honestly and he/she can launch an attack with the aid of the anonymous mechanism. Namely, the driver, as an adversary, would like to maximize his/her interest when making the parking space reservation. Despite the fact that the vehicle only needs a parking space, it could pretend to be many vehicles and preoccupy all possible parking space in the nearby parking lots. Under such condition, it is very difficult for the PSP to detect and track the attack due to the anonymity if no trusted third party exists.

In this paper, to address the above-mentioned challenges in the parking reservation scenario, we propose a novel privacy-preserving reservation scheme for securing AVP system, which can protect the users' privacy using cryptographic techniques and prevent the "Double-Reservation Attack" in a simple but efficient way. The fundamental intuition of our scheme is to design a mechanism which makes sure that each anonymous user must have only one valid reservation token at any moment, and the token can only be used for booking one vacant parking space once. The contributions of this paper are summarized as twofolds.

- We define the system and security model for a reservation/parking case of an AVP system without a trusted third party. Following the models, we propose a privacy-preserving parking reservation scheme based on four building blocks: zero-knowledge proofs of knowledge, geo-indistinguishable mechanism, proxy re-signature, and bloomfilter data structure. The proposed scheme does not only protect the driver's identity privacy and location privacy, but also prevents the "Double-Reservation Attack".
- The extensive simulation shows that our scheme's performance is better than the existing schemes [8]–[10] in terms of computational costs, communication overheads and storage costs. Additionally, a WiFi-based testbed is established and our scheme is efficient and practical under wireless channels and the smartphone environment.

The remainder of this paper is organized as follows. In Section II, we introduce the system model, security model and design goals. Then, we propose our privacy-preserving reservation scheme in Section III. Subsequently, security analysis and performance evaluation are shown in Section IV and Section V, respectively. Finally, Section VI reviews some related works and Section VII draws the conclusion.

II. Models and Design Goal

In this section, we define the system model, security model, and also identify the design goal for a reservation/parking case of an AVP system.

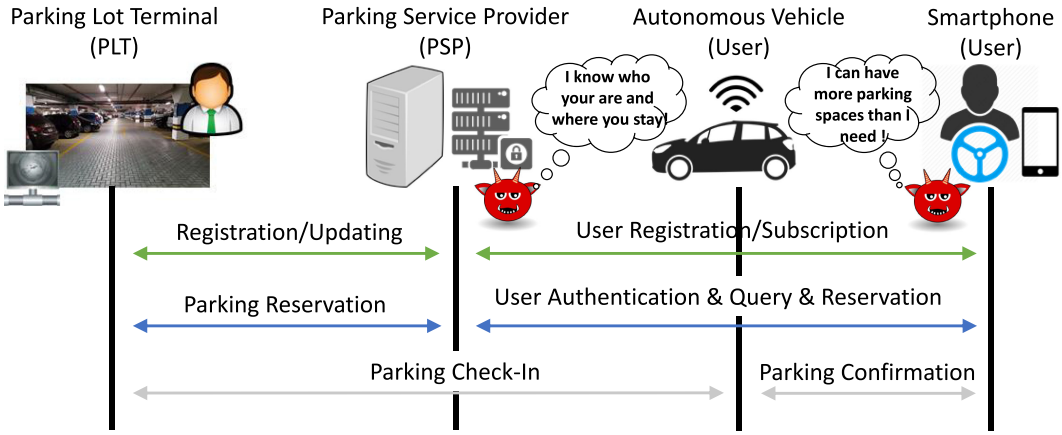


Fig. 3. A system model of reservation and parking case for AVP.

A. System Model

Our system model mainly consists of the following four entities: the parking lot terminal (PLT), the parking service provider (PSP), the autonomous vehicle (AV), and the smartphone (SM) as shown in Fig. 3.

- **Autonomous Vehicle (AV)**: The AV is a critical and mobile component for an AVP system. With the support of self-driving techniques, smart vehicles can achieve automated parking operations. The AV is supposed to have an autonomous capability (can be low-level to high-level depending on different situations) in automated driving and parking modes, and also has a communication ability based on cellular network (e.g. LTE V2X [11]) so that it can be directly connected with other entities in the network. The AV is owned by and under the control of a driver (a.k.a user), and the user could command the AV to accomplish some tasks, such as self-parking.
- **Smartphone (SM)**: The SM is an intelligent portable device, which has a restricted computational capability and is bound with the AV. Obviously, any well-designed smartphone is able to communicate with others through the internet (e.g., WiFi). The SM is owned by and under the control of a driver (a.k.a user), and the user could install the parking application and use this application to complete the reservation process.
- **Parking Service Provider (PSP)**: The PSP is a group of online servers that provide the on-demand parking service for the users, involving finding nearby parking space, making parking space reservation and other superior services. These services, offered by a parking management company, are the subscription services. Only the registered user who pays the membership fee can enjoy these convenient services. Furthermore, the services could be published to the users as a smartphone application, like an Android/IOS App.
- **Parking Lot Terminal (PLT)**: The PLT is a terminal deployed by the owner of the parking lot, which is responsible for monitoring and managing the parking lot through IoT devices (e.g. cameras and sensors), such as recording the parking space status and charging the fee for the parking car. In addition, the PLT will upload its parking lot's real-time status (e.g. the parking fee, the unoccupied parking space and the high-definition map) to the PSP so as to attract more vehicles. Meanwhile, the PSP could utilize this information for the parking lot recommendation.

To clearly illustrate a reservation and parking case, only one type (reservation then parking) of AVP parking services is discussed in detail, in this paper as shown in Fig. 3. Above all, the users should download the parking App in their SMs and register themselves at the PSP. Moreover, the valid parking lots' public information is collected by the PSP in real time. When a user intends to find a parking space, he/she first needs to pass the authentication as a registered subscriber using the installed App, and then queries based on his/her current location and makes a parking space reservation according to his/her requirements. Finally, the user will let his/her AV check in and park at the reserved space by communicating with the AV through the SM, and gets the confirmation when the parking process is over. We omit the picking-up process for a parking service since it is beyond the scope of this paper.

B. Security Model

The PSP is *honest-but-curious*, i.e., it follows the protocols, but is also curious about the user's privacy by launching passive attacks. We give an explicit definition of the user's privacy for the autonomous valet parking service at the intuitive level. Specifically, we desire our privacy-preserving reservation scheme to have the following two properties to protect the user's identity privacy:

- **Pseudonymity**: The PSP will not be able to identify the unique user's real identity that generates a particular reservation/parking request/query. The only exception is at the stage of registration, and the users have to reveal their real identities to the PSP to prove themselves as the valid users.
- **Unlinkability**: The PSP cannot correlate a user's any two reservation/parking sessions. With the knowledge of two sessions' authenticated credentials, two sessions cannot be linked any better than guessing even if the they come from the same user.

Pseudonymity and unlinkability could be summarized as anonymity to some extent, which is a simple but an effective way to protect the user's identity privacy. To further enhance the user's location privacy, the property named geo-indistinguishability [12], is also utilized to protect from the location-based statistical analysis attack in our system.

- **Geo-indistinguishability**: The location obfuscation mechanism used by the users satisfies ε-geo-indistinguishability.

From another point of view, the users should not be totally trusted because they are selfish and can launch the attack driven by self-interest and gain the benefits. In our security model, the selfish users may deliberately reserve/occupy many parking spaces at once since they are anonymous and cannot be tracked, although they merely need one parking space. Therefore, we introduce this new primitive named **"Double-Reservation Attack"** in the reservation process for an AVP system.

In addition, we assume that the PLT does not collude with the PSP to compromise the user's privacy. Since this kind of collusion attack has become a physical attack, and it cannot be entirely solved based on secure protocols. Supposing that the PLT, colluding with the PSP, can use the cameras to record a user's parking AV, it would definitely approve the real identity (car's exclusive license number) of a user to the PSP, no matter what protocols are proposed to protect the user's privacy. In this situation, not only should the secure protocols be designed but also the privacy law should be applied to forbid the privacy violation behaviors of the parking company in the physical world, which is out of scope of this paper.

However, there exist two main limitations in our security model: 1) the exact probability that two pseudonyms of a user can be linked depends on various "side-information". The linking probability does not just rely on the anonymity but also the user's requirements and behaviors. These "side-information" could be linked to identify the unique human [7]. Nevertheless, note that the common parking issues always happen in the most populous regions (a lot of vehicles needs to be parked nearby and cannot easily find a parking space) and in a discrete way (a driver usually will not have two continuous reservation/parking requests), so there could be plenty of similar parking requests during a short period at the adjacent locations, which will help relieve this limitation; 2) there might be other ways, outside our security model, where a user's privacy can be violated. For example, the original IP address in the cellular network could be a single tag to identify the user (a.k.a, network traffic analysis). To cope with the issue, our scheme could be coupled with other techniques (e.g., the anonymous network, Tor [13]) to guarantee the user's privacy.

C. Design Goal

Under the aforementioned system model and security model, our design goal is to propose a privacy-preserving reservation scheme for autonomous valet parking. In particular, the following four objectives should be achieved:

- **Privacy**: The user's privacy can be protected, i.e., when a user reserves a vacant parking space through the PSP, the PSP cannot identify the user's real identity and cannot link one user's continuous parking reservation requests at different time intervals.
- **Resistance to Double Reservation Attack**: The reservation system must resist to the "Double-Reservation Attack", i.e., the PSP only allows the user to book one parking space at one time and does not allow one user to make multiple reservations and occupy unlimited parking spaces at the same time.
- **Functionality**: The basic functions supporting reservation for an AVP system should be achieved. The basic functions cover user subscription, user authentication and parking reservation/cancelling, etc.
- **Efficiency**: The proposed scheme should be efficient in terms of computational overheads, communication and storage costs at both user side and PSP side. To implement the reservation scheme for a real-world AVP system, both the security and efficiency issues should be considered to locate a trade-off solution.

TABLE I
NOTATIONS FREQUENTLY USED IN OUR SCHEME

Notation	Definition
λ	the security parameter
$\mathbb{G}$,$\mathbb{G}_T$	two cyclic multiplicative groups
p	a large prime whose length is λ
g	a generator of $\hat{\mathbb{G}}$
$H(), H'(), \hat{H}()$	three non-cryptographic hash functions
$(a, A = g^a)$	the PSP's private key and public key
X, Y, Z	$X = g^x$, $Y = g^y$, $Z = g^z$ and $x, y, z \in Z_p$
$e(.,.)$	a non-degradable bilinear mapping
μ	the daily verification day
Ω, Ξ, Ψ	three sets for storage
(B, g^b)	the PLT's private key and public key
R_{ab}	the PLT's resignature key
$cred$	the anonymous credential of user
$Timestamp$	the current timestamp
$SESS$	the token of each parking session

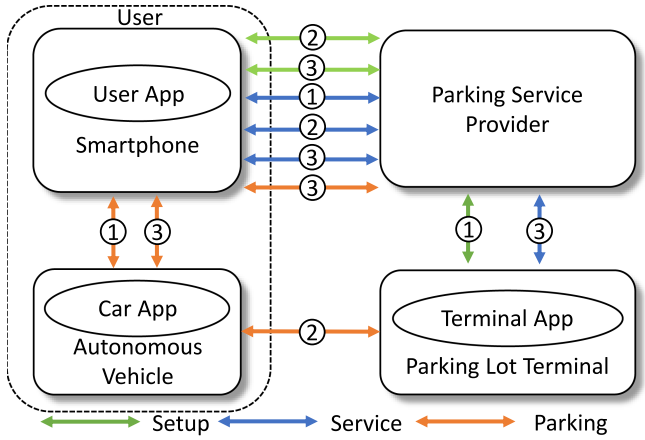


Fig. 4. The communication framework of AVP.

III. THE PROPOSED SCHEME

In this section, we first define the pieces of our privacy-preserving reservation scheme and then present a construction for the proposed scheme based on four basic building blocks: zero-knowledge proofs of knowledge [14], geo-indistinguishable mechanism [12] and proxy re-signature [15], and bloomfilter data structure. For easier reading, we also give the description of notations to be used in our scheme in Table I.

A. Design

There are three major pieces of the proposed scheme in an AVP system, as shown in Fig. 4, including **System Setup**, **Service Phase**, and **Parking Phase**.

- **System Setup**: ① the PLT registers itself at the PSP, and updates its real-time parking condition for the PSP periodically; ② the user registers himself/herself at the PSP; ③ the registered user subscribes to the services based on the online payment, such as Alipay or Paypal, and acquires the anonymous subscriber credential by smartphone.
- **Service Phase**: ① the user authenticates himself/herself to the PSP as a registered subscriber via smartphone; ② the user queries and searches the nearby parking lots for the vacant parking spaces, and then choose one vacant parking space according to the requirements; ③ the user sends the reservation request to the PSP and the PSP makes the parking reservation at the PLT, and then the parking permit generated by the PLT is sent back to the user.
- **Parking Phase**: ① the user forwards the permit to the AV by smartphone and commands the AV to park at the reserved parking space in an autonomous driving model; ② the AV checks into the parking lot based on the permit and fetches the confirmation receipt; ③ the AV forwards the receipt to the user via communication with the SM and the user renews the anonymous subscriber credential at the PSP using the receipt.

B. Main Construction

For easy understanding of the construction, we denote the zero-knowledge proofs of knowledge ($ZkPoK$), similar to [16], where a prover convinces a verifier of knowledge of values $(a_1, \ldots, a_n)$ that satisfy the predicate $\mathbb{P}$ by

$$ZkPoK\{(a_1, \ldots, a_n)|\mathbb{P}(a_1, \ldots, a_n)\}.$$

We also denote the geo-indistinguishable mechanism on the location-based query data (lat, lon, rng) as the function $\mathcal{DP}(lat, lon, rng, \varepsilon)$, where lat, lon are coordinates, rng is the query range and ε is the privacy-related parameter, which is similar to [17]. The details will be discussed later.

1) System Setup: **(Offline Setup)** the PSP runs the setup algorithm. Bilinear map groups $(\mathbb{G}, \mathbb{G}_\mathbb{T})$ of a prime order $p > 2^\lambda$ are created, where λ is the security parameter and $e(.,.)$ denotes the bilinear map such that $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_\mathbb{T}$. Formally, g is a generator of $\mathbb{G}$ and $e(g, g)$ is defined as g_T. $H : \{0,1\}^* \to Z_p$, $H' : \{0,1\}^* \to \mathbb{G}$, and $\hat{H} : Z_p \to Z_p$ are three cryptographic hash functions, and the PSP's public key is set as $A = g^a$ for a random $a \in Z_p$ and a is the private key. Also, the PSP selects $x, y, z \in Z_p$ and computes $X = g^x$, $Y = g^y$ and $Z = g^z$. $\mu \in Z_p$ is a daily verification key chosen by the PSP. Then, the tuple $\{\mathbb{G}, \mathbb{G}_\mathbb{T}, p, g, g_T, e, X, Y, Z, H, H', \hat{H}, \mu, A\}$ is published as the common parameters in the system. Finally, the PSP initializes three empty sets using bloomfilter $\Omega = \{\emptyset\}, \Xi = \{\emptyset\}$ and $\Psi = \{\emptyset\}$. Note that, μ, Ω, Ξ and Ψ are reseted per day by the PSP, indicating that the user's anonymous credential is only valid for daily period.

① **PLT Registration**: (1.1) the PLT creates a username and password, and registers itself in the terminal; (1.2) the PLT uploads the identity information, such as the electronic commercial parking lot license, to the PSP, and the PSP verifies the qualification of the parking lot; (1.3) once the verification has been passed successfully, the PLT creates a key pair as $(B = g^b, b)$ where b is chosen randomly over Z_p, calculates the resignature key $R_{ab} = A^{\frac{1}{b}} = g^{\frac{a}{b}}$ and sends the public key B to the PSP; (1.4) the PSP stores B, the parking lot information and completes the registration.

② **User Registration**: (2.1) the user creates a username and password, and registers itself in the user App; (2.2) the user uploads the identity information, such as the electronic driving license, to the PSP, and the PSP verifies the qualification of the user; (2.2) once the verification has been passed successfully, the user finishes the registration.

③ **User Subscription**: (3.1) the user logins into the user App via the valid username and password, and pays the service fee online; (3.2) Once the payment is confirmed by the PSP, the user chooses $(d, r) \in Z_p^2$, constructs $M = Y^d Z^r$, and sends $(M, \hat{H}(d))$ to the PSP; (3.3) the PSP checks whether $\hat{H}(d)$ exists in Ω. If it exists, the PSP guides the user to go back to the step (3.2). Otherwise the PSP adds $\hat{H}(d)$ into Ω; (3.4) the user acts as prover and the PSP as verifier in the zero-knowledge proof of knowledge:

$$ZkPoK\{(d, r)|M = Y^d Z^r\};$$

(3.4) the PSP returns as failure if the proof fails. Otherwise the PSP sends to the user a tuple (W, v), where $v \in Z_p$ and $W = (XM)^{\frac{1}{v+a+\mu}}$; (3.5) the user checks whether $e(W, Ag^{v+\mu}) \stackrel{?}{=} e(XM, g)$. If it fails, the user returns as failure. Otherwise the anonymous credential is stored as $cred = (W, v, d, r)$ locally.

To avert losing the anonymous credential incidentally and support credential recovery, $cred$ is encrypted using a preset secret password $pass$ chosen by the user as $E_{pass}(cred)$, and $E_{pass}(cred)$ can be stored online at the PSP, where $E()$ is a common symmetric encryption algorithm, such as AES.

2) Service Phase: ① **User Authentication**: (1.1) the user acts as prover and the PSP as verifier in the zero-knowledge proof of knowledge:

$$ZkPoK\{(W, v, d, r)|W^{v+a+\mu} = XY^d Z^r\},$$

and logins to the PSP via the App; (1.2) if the proof is successful, the PSP generates a unique temporary session token $SESS$, and sends it back to the user. Otherwise the PSP returns as failure; (1.3) the user stores the session token $SESS$.

② **Parking Query**: (2.1) the user's current location-based query (lat, lon, rng) is noised by utilizing the geo-indistinguishable mechanism as

$$(lat', lon', rng') = \mathcal{DP}(lat, lon, rng, \varepsilon);$$

(2.2) the user sets the parking requirements and requests the neighbour parking lot information by sending (lat', lon', rng') and $SESS$ to the PSP; (2.3) the PSP filters the parking lots that do not meet the criteria and returns the parking lots list within the query range.

③ **Parking Reservation**: (3.1) the user selects a parking lot from the returned list, sends the reservation request Req to the PSP, where $Req = Info||SESS||Timestamp$ ($Info$ involves the trivial reservation information and $Timestamp$ indicates the current timestamp); (3.2) the user calculates $U = g^{\frac{1}{d+\mu}}$ as the booking token, sends U to the PSP and engages in a zero-knowledge proof of knowledge with the PSP, in which the user plays the prover, the PSP plays the verifier:

$$ZkPoK\{(W, v, d, r)|W^{v+a+\mu} = XY^d Z^r \wedge U = g^{\frac{1}{d+\mu}}\};$$

(3.3) after receiving the request, if the proof succeeds and the token U does not exist in Ξ, the PSP accepts the request and

adds U into Ξ. Otherwise the PSP rejects the request; (3.4) the PSP signs the request as $\sigma = H'(Req)^a$ and relays the request $Req||\sigma$ to the corresponding PLT; (3.5) the PLT verifies the signature of the request by checking

$$e(\sigma, g) \stackrel{?}{=} e(H'(Req), A).$$

If it fails, the reservation request is rejected. Otherwise the PLT generates a unique random string as the temporary parking permit code c, stores it in its local database, and also sends it back to the PSP; (3.6) the PSP signs c as $Sig_c = H'(c||Timestamp||SESS)^a$, stores $SESS$ in its token pool, and gives $c||Sig_c$ back to the user; (3.7) the user verifies the signature Sig_c by checking

$$e(Sig_c, g) \stackrel{?}{=} e(H'(c||Timestamp||SESS), A).$$

If it is valid, the user stores $c||Timestamp||SESS||Sig_c$.

Moreover, the user can cancel the current parking/reservation session if necessary by sending the session token $SESS$ and the booking token U to the PSP with a reservation canceling request. After receiving the canceling request, the PSP will delete the parking reservation record and notifies the corresponding PLT. The user can then use the same session token U to renew his/her anonymous credential, following the steps in **User Subscription** except the step (3.1).

3) Parking Phase: ① **Parking Request**: (1.1) the user relays $c||Timestamp||SESS||Sig_c$ and the parking lot information to the AV via the SM; (1.2) the AV switches to the self-driving mode and drives to the selected parking lot according to the received information.

② **Parking Check-In**: (2.1) when connecting to the PLT, the AV sends $c||Timestamp||SESS$ to the PLT; (2.2) the PLT verifies the signature Sig_c by checking

$$e(Sig_c, g) \stackrel{?}{=} e(H'(c||Timestamp||SESS), A).$$

If it is valid, the PLT searches c in its database and assures that whether the AV has already reserved a parking space or not. If c is found in its local database, the PLT deletes c and allows the AV to park inside. Otherwise the PLT returns as failure and refuses to offer the service; (2.3) the PLT re-signs Sig_c by choosing a random $\theta \in Z_p$ as $Sig'_c = (Sig_c^\theta, A^\theta, R_{ab}^\theta)$, and transmits Sig'_c as the confirmation receipt to the AV.

③ **Anonymous Credential Renewal**: (3.1) the AV forwards the receipt Sig'_c to the user's SM and notifies the parking confirmation message on the user's SM; (3.2) After waiting for a random delay, the user applies for a new anonymous credential by sending $c||Timestamp||SESS||Sig'_c||U$ to the PSP; (3.3) after receiving the renewal request, the PSP checks the validity of the credential renewal request by the following three conditions.

- **(Condition.1)** The PSP searches the session token $SESS$ in the session token pool. If $SESS$ exists, the PSP deletes it and this condition is satisfied.
- **(Condition.2)** The PSP verifies the signature Sig'_c by the following equations.

$$e(Sig_c^\theta, g) \stackrel{?}{=} e(A^\theta, H'(c||Timestamp||SESS)),$$
$$e(A^\theta, g) \stackrel{?}{=} e(B, R_{ab}^\theta).$$

If the equations hold, this condition is satisfied.

- **(Condition.3)** The PSP searches U in Ξ and Ψ. If U exists in Ξ and does not exist in Ψ, the PSP adds U into Ψ and this condition is satisfied.

If any of them are not fulfilled, the PSP rejects the request and returns as failure. Otherwise, the PSP returns with success; (3.4) the user gains a new anonymous credential, following the steps in **User Subscription** except the step (3.1).

In addition, to deal with the issue that some important messages, such as the acknowledgment of the parking space, may be lost at the user side accidentally, our scheme relies on the PSP as the intermediate servers to store this information. If the users miss the acknowledgment, the PSP can help the user check and download this missing information based on the user's temporary session token. Since the temporary session token is unique and only known by the user and the PSP, only the authorized anonymous user who has already sent this request can check the status of this reservation session. Then, there are two cases: 1) if the request is successful, the user can download the acknowledgment; and 2) if the request is not successful, the user can resend the reservation request.

C. More Details

1) Zero-Knowledge Proofs of Knowledge: We present the non-interactive zero knowledge proofs of knowledge ($ZkPoK$) that are secure in the random oracle model (Fiat-Shamir heuristic).

Proof.I $ZkPoK\{(d,r)|M = Y^d Z^r\}$:

Prover:

1) Choose $\alpha, \beta \in Z_p$, calculate $\Delta = Y^\alpha Z^\beta$
2) Set $\eta = H(Y, Z, M, \Delta)$
3) Send $(\Delta, M, \hat{\alpha} = d\eta + \alpha, \hat{\beta} = r\eta + \beta)$ to the verifier

Verifier:

1) Calculate $\eta = H(Y, Z, M, \Delta)$
2) Check that $M^\eta \Delta = Y^{\hat{\alpha}} Z^{\hat{\beta}}$

Proof.II $ZkPoK\{(W, v, d, r)|W^{v+a+\mu} = XY^d Z^r \wedge U = g^{\frac{1}{d+\mu}}\}$:

Note that, the proof can be transformed and rewrited [18] as

$$ZkPoK\{(v, d, r, \alpha_1, \alpha_2, \beta_1, \beta_2)|W_1 = Y^{\alpha_1} Z^{\alpha_2} \wedge$$
$$1_{\mathbb{G}} = W_1^{-v} Y^{\beta_1} Z^{\beta_2} \wedge U^d = gU^{-\mu} \wedge \frac{e(W_2, Ag^\mu)}{e(X, g)}$$
$$= e(W_2, g)^{-v} e(Y, g)^d e(Z, A)^{\alpha_1} e(Z, g^u)^{\alpha_1} e(Z, g)^{r+\beta_1}\}$$

where $\alpha_1, \alpha_2 \in Z_p$, $W_2 = WZ^{\alpha_1}$, $\beta_1 = \alpha_1 v$, and $\beta_2 = \alpha_2 v$.

Prover:

1) Choose $\rho_v, \rho_d, \rho_r, \rho_{\alpha_1}, \rho_{\alpha_2}, \rho_{\beta_1}, \rho_{\beta_2} \in Z_p$, calculate $\Delta_1 = Y^{\rho_{\alpha_1}} Z^{\rho_{\alpha_2}}$, $\Delta_2 = W_1^{-\rho_v} Y^{\rho_{\beta_1}} Z^{\rho_{\beta_2}}$, $\Delta_3 = U^{\rho_d}$, $\Delta_4 = e(W_2, g)^{-\rho_v} e(Y, g)^{\rho_d} e(Z, A)^{\rho_{\alpha_1}} e(Z, g^\mu)^{\rho_{\alpha_1}} e(Z, g)^{\rho_r + \rho_{\beta_1}}$
2) Calculate $\eta = H(X, Y, Z, W_1, W_2, U, \Delta_1, \Delta_2, \Delta_3, \Delta_4)$
3) Send $(\Delta_1, \Delta_2, \Delta_3, \Delta_4, W_1, W_2, U, \hat{\rho_v} = v\eta + \rho_v, \hat{\rho_d} = d\eta + \rho_d, \hat{\rho_r} = r\eta + \rho_r, \hat{\rho_{\alpha_1}} = \alpha_1\eta + \rho_{\alpha_1}, \hat{\rho_{\alpha_2}} = \alpha_2\eta + \rho_{\alpha_2}), \hat{\rho_{\beta_1}} = \beta_1\eta + \rho_{\beta_1}, \hat{\rho_{\beta_2}} = \beta_2\eta + \rho_{\beta_2})$ to the verifier

Verifier:

1) Calculate $\eta = H(X, Y, Z, W_1, W_2, U, \Delta_1, \Delta_2, \Delta_3, \Delta_4)$
2) Check that $W_1^\eta \Delta_1 = Y^{\hat{\rho_{\alpha_1}}} Z^{\hat{\rho_{\alpha_2}}}$, $1_{\mathbb{G}}{}^\eta \Delta_2 = W_1^{-\hat{\rho_v}} Y^{\hat{\rho_{\beta_1}}} Z^{\hat{\rho_{\beta_2}}}$, $(gU^{-\mu})^\eta \Delta_3 = U^{\hat{\rho_d}}$, and $(\frac{e(W_2, Ag^\mu)}{e(X, g)})^\eta \Delta_4 = e(W_2, g)^{-\hat{\rho_v}} e(Y, g)^{\hat{\rho_d}} e(Z, A)^{\hat{\rho_{\alpha_1}}} e(Z, g^\mu)^{\hat{\rho_{\alpha_1}}} e(Z, g)^{\hat{\rho_r} + \hat{\rho_{\beta_1}}}$

2) Geo-Indistinguishable Mechanism: Given the parameter $\varepsilon \in \mathbb{R}^+$ (i.e., the default privacy levels can be set as low $\varepsilon = 0.01$, medium $\varepsilon = 0.004$, and high $\varepsilon = 0.001$), and the actual location $pos = (lat, lon) \in \mathbb{R}^2$, the probability density function of noise mechanism (planar Laplacian), on any other point $pos = (lat', lon') \in \mathbb{R}^2$, is $D_\varepsilon(pos)(pos') = \frac{\varepsilon^2}{2\pi} e^{-\varepsilon d(pos, pos')}$, where d denotes the Euclidean distance. It can also be represented as polar coordinate model $D_\varepsilon(rad, \theta) = \frac{\varepsilon^2}{2\pi} \cdot rad \cdot e^{-\varepsilon \cdot rad}$, where rad and θ are distance and angle with respect to pos. To obfuscate the real location, specifically, θ should be uniformly chosen from $[0, 2\pi)$ and rad should be set as $rad = C_\varepsilon^{-1}(p) = -\frac{1}{\varepsilon}(W_{-1}(\frac{p-1}{e}) + 1)$, where W^{-1} is the Lambert W function (the -1 branch) and p should be uniformly chosen from $[0, 1)$. Also, two transformation functions are needed: LatLonToCartesian and CartesianToLatLon, to transform $(lat, lon) \rightarrow (\bar{x}, \bar{y})$ and $(\hat{x}, \hat{y}) \rightarrow (lat', lon')$. Therefore, $\hat{x} = \bar{x} + rad \cdot \cos\theta$ and $\hat{y} = \bar{y} + rad \cdot \sin\theta$. In addition, $rng' = rng - \frac{1}{\varepsilon}(W_{-1}(\frac{\tau-1}{e}) + 1)$, where τ is the accuracy parameter (default $\tau = 0.95$).

3) Efficient Set Membership Test: The construction requires efficient set membership tests for three sets Ω, Ξ and Ψ, and the standard bloomfilter (BF) data structure is used properly. The characteristics of this data structure deeply match the requirements of our construction, which include the compressed storage for large dataset, the zero false negative rate, and the fast search algorithm: since the number of reservation/parking requests is large, the BF helps diminish the storage overheads; since each booking token U can only be used for one time, it could not be missed by BF if it had been used due to the zero false negative rate; the fast search algorithm can accelerate the testing speed and reduce the computational costs. Generally, a BF consists of an array of m cells, each of which is a bit with an initial value 0, and k independent random hash functions, where m and k are determined by the maximum number of data items supported by BF and the false positive ratio of BF.

IV. Privacy and Security Analysis

A. Privacy Analysis

Following the privacy requirements discussed earlier, our analysis will focus on how the proposed scheme can ensure the user's pseudonymity, unlinkability and geo-indistinguishability.

Pseudonymity: Each user has totally different anonymous credentials (W, v, d, r) for different reservation/parking sessions in our proposed scheme. The anonymous credential, as a unique pseudonym defined by the user and confirmed by the PSP (Proof.I), can be verified by the PSP as the valid anonymous credential (part of Proof.II) during the anonymous authentication process. Hence, the user's pseudonymity relies on the security of two zero-knowledge proof protocols. Specifically, Proof.I is an adapted version of the CL signature scheme [19] and Proof.II is an adapted version of the BBS/BBS+ signature schemes [18], [20]. Their security proofs are thus relatively straightforward.

Unlinkability: TAuSM08he PSP can perform the pseudonym linking attack, and our scheme guarantees that the possibility that the PSP succeeds in linking one user's two reservation/parking sessions cannot be better than guessing. In other words, the PSP cannot link the user's real identity and the user's first anonymous credential during user subscription, and the PSP cannot link the user's previous anonymous credential and renewed anonymous credential during anonymous credential renewal. This property of unlinkability is dependent on two zero-knowledge proof protocols Proof.I and Proof.II. When the user applies for the anonymous credential using his/her real identity, the PSP only knows that the registered user acquires a valid anonymous credential, it does not know the values of (d, r) but can still acknowledge the anonymous credential (W, d, v, r) (Proof.I) as a valid BBS+ signature. During parking reservation, the user's reservation token U cannot be linked to a specific anonymous credential by the PSP since the PSP does not have d. Similarly, the PSP only knows that a new anonymous credential is generated and assigned to the anonymous user during the renewal period, but it does not know the content of this new credential. During anonymous authentication, the PSP and the user run a non-interactive zero knowledge proof to verify the BBS/BBS+ signature, i.e., the PSP can verify $W^{v+a+\mu} = XY^d Z^r$ without knowing the values of (W, d, v, r), which guarantees the unlinkability.

Geo-indistinguishability: ε-geo-indistinguishability is defined as $\frac{P(Z|x)}{P(Z|x')} \leq e^{\varepsilon d(pos, pos')}$, where P is the conditional probability. Each observation is $Z \subseteq \mathcal{Z}$, where $\mathcal{Z}$ is a set of possible reported locations, and $d(pos, pos')$ is the Euclidean distance between pos and pos'. By adding a planar laplacian noise $\mathcal{N} = (rad, \theta)$ to the original location (lat, lon) in the proposed scheme, the reported location can be viewed as an obfuscated location $pos' = (lat', lon')$, and the ε-geo-indistinguishability is satisfied. The detailed proof can be found in [12].

B. Security Analysis

We focus on how the proposed scheme can be resilient to the *"Double-Reservation Attack"* in the security analysis. The proposed scheme is designed based on the idea of generating one-time booking token for each registered user and his/her every booking/parking session. To prevent the attack, the fundamental intuition is to make sure that each anonymous user should and must have only one valid token at one time. In specific, each user can obtain the token in two stages: user subscription and anonymous credential renewal. The PSP can easily assure that each registered user only applies for one anonymous credential during user subscription. If the user has been allocated the anonymous credential, other similar requests will be dropped since the account information will be recorded. For the renewal process, the situation becomes complex but can still be addressed based on three decision conditions:

- **(Condition.1)** The renewal request comes from a current reservation/parking session by checking the session token $SESS$.
- **(Condition.2)** The verification of a PLT's confirmation receipt guarantees that the anonymous user's parking session is accomplished by checking the signature Sig'_c.
- **(Condition.3)** The booking token U has already been used for booking and has not been used for renewing by performing set membership tests in Ξ and Ψ. Proof.II indicates that the token U is authenticated by the PSP, i.e., the token cannot be forged.

With the aforementioned three conditions, the PSP can update the user's exclusive anonymous credential. Namely, the attack has been prevented. The abnormal timestamp information for each reservation/parking session (i.e., time duration between reservation and parking is too short) may help detect the suspicious PLT who may collude with the malicious user even though this collusion attack gains no benefit for the attackers.

TABLE II
TESTBED SETTING

Role	Machine	Hardware and Software
PSP	Workstation	Intel i7-6700K @ 4.00 GHZ; 32 GB memory; Windows 10
PLT	Notebook	Intel Core i5-7200U @ 2.60 GHz; 16 GB memory; Windows 10
AV	Galaxy S4	1.9 GHz Krait 300; 2 GB memory; Android 5.0
Smartphone	Galaxy S4	1.9 GHz Krait 300; 2 GB memory; Android 5.0

In addition, since the parking reservation is a paid service, the proposed scheme also guarantees that only the premium users who paid the fees can use this service. The daily verification key μ, included in each user's anonymous credential and reservation token, makes sure that each user needs to refresh his/her subscription information everyday. If the subscription is expired, he/she will not be allowed to apply for a valid anonymous credential.

V. PERFORMANCE EVALUATION AND IMPLEMENTATION

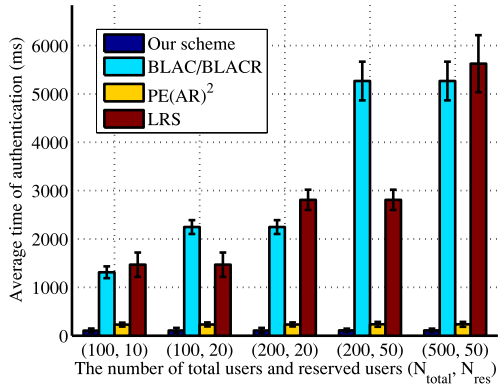
In this section, we evaluate the performance of the proposed scheme in terms of communication overheads, computational and storage costs. Also, a WiFi-based testbed has been built to further demonstrate the scheme's practicality.

A. Simulation Settings

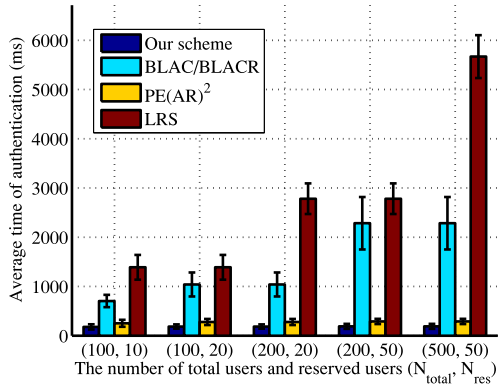
In our simulation, we compare our solution with three traditional solutions based on the blacklistable anonymous credential (BLAC/BLACR) [9], the blacklistable anonymous credential with universal accumulator (PE(AR)^2) [8] and linkable ring signature (LRS) [10], which could also deal with the "Double-Reservation Attack" anonymously under some conditions. This simulation is built on a JAVA-based simulator and conducted on a notebook with Intel Core i5-7200U CPU@2.60 GHz and 16.00 GB memory. Then, we test the scheme's performance in a testbed of one workstation, one notebook and one Android phone. These machines play the roles of the PSP, the PLT, the AV and smartphone, respectively. The hardware and software of these machines are shown in Table II.

B. Performance Comparisons

Since our solution is particularly proposed for the AVP system, it has many characteristics which the previous protocols do not have (e.g., location obfuscation at user side and the participation of PLT). Hence, we mainly investigate performance comparisons of the **anonymous authentication costs** (i.e., **the costs of parking reservation**), which involves the communication overheads, computational and storage costs. For the BLAC/BLACR-based solution, each user owns a anonymous credential after finishing payment, and the PSP maintains an anonymous blacklist. When a user reserves a vacant parking space via the PSP, he/she has to prove to the PSP (one by one) that he/she is not shown on that anonymous blacklist. When the reservation is finished, his/her anonymous credential is added to the blacklist to prevent the "Double-Reservation Attack". For the PE(AR)^2-based solution, the procedure is similar to that of



(a) Computational costs at user side



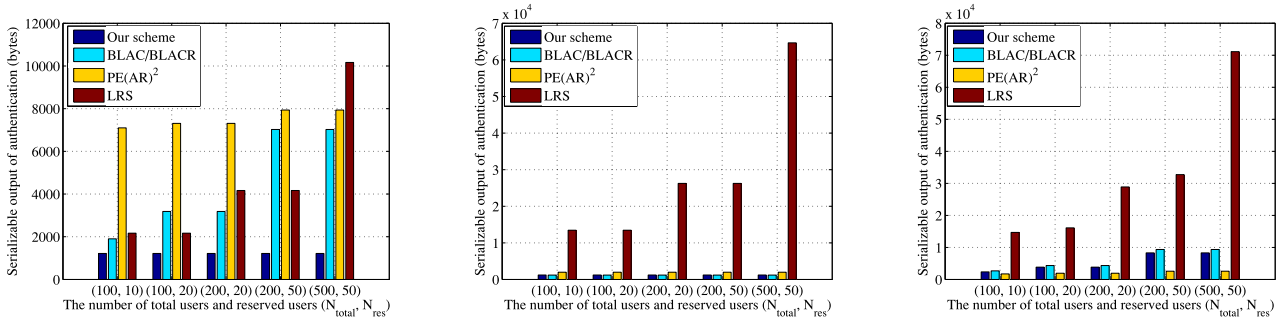
(b) Computational costs at PSP side

Fig. 5. Computational costs compared with the existing schemes.

the BLAC/BLACR-based solution, while the difference is that the proof between the user and the PSP is designed based on a universal accumulator to improve the computational efficiency for both sides. For the LRS-based solution, each user owns a unique ring signature to represent his/her identity in a predefined group. When a user books a vacant parking space via the PSP, he/she has to generate a ring signature, which indicates that he/she is from this group but conceals the specific identity, and submits this signature to the PSP. When the reservation is finished, his/her current reservation request can be linked by the PSP to the future requests to identify whether these two requests come from the same user in the group anonymously.

We use the BouncyCastle library and JAVA Pairing-Based Cryptography (JPBC) library to implement the cryptographic building blocks in our simulator. The elliptic curve of the bilinear pairing is chosen with a base field size of 512 bits and the order p is 160 bits. To keep the consistency, the simulation is conducted under the same setting. The number of total users N_{total} is set as $\{100, 200, 500, 10000\}$, and the number of reserved users (the user has finished the reservation but not achieved parking yet) N_{res} is set as $\{10, 20, 50, 1000\}$ in our simulation. The numerical results of computational costs are shown in Fig. 5, and the results are averaged by 100-times simulations.

Apparently, the execution time of BLAC/BLACR-based and LRS-based solutions are linearly increased with the growth of N_{res} and N_{total} respectively, but the running time of our scheme and PE(AR)^2-based solution is not impacted by either of them



(a) Communication overheads between user and PSP (uplink and downlink)

(b) Storage costs at user side

(c) Storage costs at PSP side

Fig. 6. Communication overheads and storage costs compared with the existing schemes.

(i.e., our scheme's execution time is almost fixed 110 ms and 180 ms at user side and PSP side, and the PE(AR)^2-based solution's execution time is almost fixed 240 ms and 260 ms at user side and PSP side). The reason is that, our scheme just requires the user to provide a one-time reservation token during each anonymous authentication process which is very efficient. However, since BLAC/BLACR requires each user to retrieve the whole blacklist and to prove to the PSP separately that he/she does not exist in that list, the proof should be executed N_{res} times between the user and the PSP (i.e., the running time of BLAC/BLACR is almost 101.211 s and 41.332 s at user side and PSP side when $N_{res} = 1000$). In another way, LRS requires each user to sign the signature on behalf of the whole group to preserve the anonymity, which indicates that the signature should involve N_{total} group member information (i.e., the execution time of LRS is almost 147.429 s and 146.873 s at user side and PSP side when $N_{total} = 10000$) and cannot be distinguished by the PSP. Although the PE(AR)^2-based solution is almost equally efficient as our scheme, it still costs more time because the user has to re-generate the accumulated witness and perform a more complex proof on during each anonymous authentication, which are not necessary in our scheme. We also give the error bars which indicate the time out and help the users to determine whether they have lost the messages to some extent. In addition, we compare the communication overheads and storage costs among our scheme, the BLAC/BLACR, the PE(AR)^2 and the LRS, and the numerical results are shown in Fig. 6. Note that, the communication overheads (uplink and downlink) and storage costs are the serializable output as the byte array type in our JAVA-based simulator, and may be different from other programming languages due to diverse data types.

The Fig. 6(a) shows that our scheme only requires around 1200-byte bandwidth per request but both the BLAC/BLACR and LRS needs more than 2000-byte bandwidth even if there are only 100 users and 10 reserved users in the system. Especially, the PE(AR)^2-based solution requires more than 7000-byte bandwidth during anonymous authentication since it has five zero knowledge proofs for every request. When $N_{total} = 10000$ and $N_{res} = 1000$, the bandwidth requirements are significantly large (i.e., each user uploads 295275 bytes for the BLAC/BLACR, 27884 bytes for the PE(AR)^2, and 200129 bytes for the LRS). Here, the BLAC/BLACR-based solution needs more bandwidth than the LRS-based solution because the user has to download the newest blacklist before any authentication takes place, and the blacklist changes as long as the parking reservation happens. Hence, the blacklist downloading overheads cannot be avoided. However, the PE(AR)^2 has a better performance than the BLAC/BLACR and the LRS when N_{total} and N_{res} is large. The reason is that the users can download the whole newest blacklist in an accumulator for the PE(AR)^2-based solution, which fills the gap of BLAC/BLACR.

For the BLAC/BLACR and PE(AR)^2, the PSP stores the blacklist and its private key, and the user stores the anonymous credential. The storage costs of LRS are decided by the number of group members (users). If there are more group members, the user has to store not only his/her key pairs but also other member's public keys, and the PSP needs to store all group members' public keys and reserved users' signatures. In our scheme, the user stores the anonymous credential, and the PSP stores its private key and three sets (i.e., the efficient bloom-filter data structure is not considered in the comparison for the sake of fairness). Although the storage costs of our scheme are not the best one compared to that of the previous solutions, the Fig. 6(b) and (c) show that the costs are still small enough to support scalability. In the real world, there may exist more than 10000 users and 1000 reserved users in the system, the storage costs of our scheme are also acceptable (1205 bytes and 148889 bytes at user side and PSP side). The BLAC/BLACR's costs are 1185 bytes and 167724 bytes, the PE(AR)^2 costs are 1973 bytes and 22529 bytes, and the LRS's costs are 1280653 bytes and 1408741 bytes at user side and PSP side.

C. Implementation on Testbed

The PSP, PLT and the smartphones are connected via WiFi, and the communication among them is designed based on the JAVA socket programming. For simplicity, the automated vehicle and smartphone at user side are programmed into one android application, while the PSP and PLT own separated JAVA server applications, which support multiple threads. The information of registered users and PLTs are store in the MySQL database which is deployed at PSP side. As shown in Fig. 7, the android application supports basic functions, such as user registration, user login, user subscription (after user login) anonymous login (i.e., user authentication), parking query (after anonymous login), parking reservation (after parking query), parking check-in (including parking request) and anonymous credential renewal. As a research demo, just one PLT application is deployed with the fixed information near the University of Waterloo, and a single PLT registration application is developed,

TABLE III
THE PERFORMANCE (DELAY) OF OUR TESTBED FOR THREE PHASES IN OUR SCHEME

Setup Phase		Service Phase		Parking Phase	
Subphase	Time	Subphase	Time	Subphase	Time
PLT Registration	$\approx$ 300 ms	**User Authentication**	$\approx$ 2 s	Parking Request	$\approx$ 100 ms
User Registration	$\approx$ 100 ms	Parking Query	$\approx$ 100 ms	Parking Check-In	$\approx$ 150 ms
User Subscription	$\approx$ 2 s	**Parking Reservation**	$\approx$ 3 s	Anonymous Credential Renewal	$\approx$ 2 s

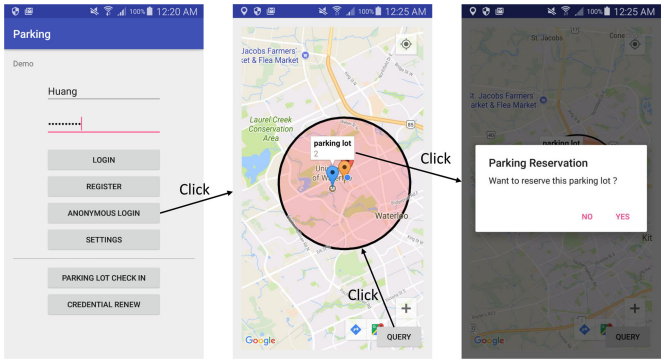


Fig. 7. Selected android client interfaces when making the parking reservation.

but it is still enough to test the performance of our scheme since multiple PLTs will not impact the performance from a design standpoint. The test results are shown in Table. III. Most of the delays are measured from the android client side, starting from the request generation to the operation completion. The most time-consuming operation of our scheme is the parking reservation which costs almost 3 seconds. User subscription, user authentication and anonymous credential renewal cost around 2 seconds, while other operations cost less than 300 ms. Therefore, our scheme is very efficient in the WiFi-based testbed.

VI. RELATED WORKS

In this section, some related works fall into three categories: (1) automated valet parking system; (2) some cryptographic techniques that may provide privacy protection and also be resilient to the "Double-Reservation Attack" with some modifications, though none of them is designed for the AVP system; (3) other privacy-preserving schemes proposed for reservation/parking applications in the vehicular networks.

A. Automated Valet Parking

Automated valet parking has the potential of becoming one of the first mature automated driving applications [4] and many research projects aim at this direction such as the V-Charge project [1] and the AutoPLES project [21]. There exist plenty of research papers in this area recently, the topics include but not limited to: high-definition 3D map generation [1], localization [22], perception/environment model [23] and motion planning [24]. For example, Schwesinger *et al.* [1] leveraged multi-camera SLAM to simultaneously build the real-time environmental 3D map. Ibisch *et al.* [22] proposed a localization method by deploying the environment-embedded LIDAR sensors in the parking garage. Bertozzi *et al.* [23] proposed a detection and tracking algorithm using 4 fisheye cameras, which is able to detect and track moving pedestrians and vehicles. Gonzalez *et al.* [24] reviewed the previous works on motion planning, which are designed based on various policies, including graph search, sampling, and interpolating curve and numerical optimization. Note that, the above works focus on the functionality of AVP system but not the security and privacy issues, which is another obstacle to the deployment of AVP system.

B. Cryptographic Techniques

A typical technique for addressing the "Double-Reservation Attack" while keeping the identity anonymous is blind signature [25]. The solutions based on blind signature technique were mostly proposed for the digital cash scenario and deal with the so-called "Double-Spending" risks with the help of a third-party trusted party. In this parking case, the link operation of two double reservations should be performed on the third-party trusted server, which makes these solutions not compatible with the real-world AVP system. To make the case more flexible, two methods are proposed without the need of a trust authority: the blacklistable anonymous credential [8], [9], [26] and linkable ring (group) signature [10]. The solutions based on the blacklistable anonymous credential rely on a dynamic anonymous blacklist to identify the malicious user when authenticating that user. These solutions are effective in problem solving but pays heavy costs in terms of computational costs and communication overheads, as we simulated in Section V, part B. The solutions based on the linkable ring signature are designed based on the group signature to preserve the identity privacy while supporting linking two repetitive requests from one anonymous user in that group. However, these solutions can only satisfy partially anonymity that achieves pseudonymity but not unlinkability. Moreover, the blockchain technique is introduced in recent years, and some solutions [27], [28] based on blockchain were proposed. These solutions were under the decentralized architecture and bring new benefits, such as no single of point failure. Since the basic blockchain does not support the anonymity (only pseudonymity), these solutions need to modify the basic blockchain to guarantee both the identity and transaction privacy. Nevertheless, the new privacy-preserving blockchain protocols proposed in these solutions sacrifice more costs while considering that the original one is not efficient due to proof of work, which is difficult to judge the practicality in our AVP system.

C. Privacy-Preserving Reservation/Parking Applications

Some recent works [29]–[34] have been presented to achieve privacy-preserving parking navigation, payment and reservation based on vehicular ad hoc networks (VANETs). Lu *et al.* [30]

presented an intelligent secure and privacy-preserving parking scheme through vehicular communications. They used roadside units (RSUs) to localize vehicles and assist them to find vacant parking spaces in a privacy-preserving way, i.e., vehicles use the pseudonyms, assigned by a third-party trust authority, to protect their privacy when communicating with the RSUs. Similarly, Ni *et al.* [31] proposed a cloud-based privacy-preserving parking navigation system in VANETs to find accessible parking spots for vehicles. They utilized the anonymous credential to protect the location privacy of vehicles in VANETs. Also, in the extended version [32], they provided more details about the navigation performance analysis. Furthermore, Garra *et al.* [33] proposed a privacy-preserving pay-by-phone parking system by implementing an anonymous e-coin-based payment protocol. The proposed scheme can keep the payment information secret while providing the evidence that the payment has been finished without leaking the user's privacy. Liu *et al.* [29] proposed a privacy-preserving reservation system for electric charging stations, which is similar to our work. They relied on a trust authority to design a privacy-preserving reservation and penalty mechanism, which can also preserve the privacy between the electric vehicles and charging stations. Apparently, although some privacy-preserving parking applications have been proposed, none of them is specifically designed for the AVP system.

In addition, most of the above schemes, including our work, are designed for protecting users' privacy in the communication-based parking reservation system where all operations are done through the communication as shown in our system model. From another perspective, the vision-based parking space management system may also compromise the user's privacy when the system's cameras record the parking videos of vehicles' parking process. However, this challenge is more related to the privacy protection in the video surveillance system [35], and this challenge can be addressed by using a privacy-preserving camera [36], which comes from a different motivation. We refer the interested readers to [37] for more details.

VII. Conclusion

In this paper, we have proposed a privacy-preserving reservation scheme for securing AVP system. The security model is first presented to define the privacy requirements and the potential attacks in this system. Then, the proposed scheme has been designed particularly based on the features of AVP system, to guarantee both the user's identity privacy and location privacy, and prevent the "Double-Reservation Attack" performed by the malicious users. In the current work, a secure and privacy-preserving user-centric automated parking system is proposed. The vacant parking spaces are chosen by the drivers themselves, which makes the location privacy of any driver can be easily protected by location obfuscation mechanism. In the future work, a totally different server-centric automated parking system is considered to schedule the whole parking process of vehicles, i.e., the parking service provider makes the decisions on where to park for each vehicle. Since the consequence of location obfuscation will greatly influence the results of optimal parking scheduling, the key issue is to balance the location privacy and parking utility by analyzing the effects of different location obfuscation mechanisms.

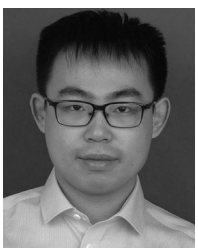
Acknowledgment

The authors gratefully acknowledge the suggestions and comments of Intel research scientist Dr. E. Liao and her team.

References

[1] U. Schwesinger *et al.*, "Automated valet parking and charging for e-mobility," in *Proc. Intell. Veh. Symp.*, 2016, pp. 157–164.
[2] D.-B. Company, "When the app parks the vehicle," 2017. [Online]. Available: https://www.daimler.com/innovation/next/when-the-app-parks-the-vehicle.html. Accessed on: Nov. 11, 2017.
[3] Z. Technology, "Zongmu showcases its first low-speed high-automation product to CES 2018," 2018. [Online]. Available: http://www.zongmutech.com/en/news/20180109378. Accessed on: Jan. 25, 2018.
[4] H. Banzhaf, D. Nienhüser, S. Knoop, and J. M. Zöllner, "The future of parking: A survey on automated valet parking with an outlook on high density parking," in *Proc. Intell. Veh. Symp.*, 2017, pp. 1827–1834.
[5] T. M. T. Do and D. Gatica-Perez, "The places of our lives: Visiting patterns and automatic labeling from longitudinal smartphone data," *IEEE Trans. Mobile Comput.*, vol. 13, no. 3, pp. 638–648, Mar. 2014.
[6] Y. He, J. Ni, X. Wang, B. Niu, F. Li, and X. Shen, "Privacy-preserving partner selection for ride-sharing services," *IEEE Trans. Vehicular Technol.*, vol. 67, no. 7, pp. 5994–6005, Jul. 2018.
[7] Y.-A. de Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, "Unique in the crowd: The privacy bounds of human mobility," *Sci. Rep.*, vol. 3, pp. 1–5, 2013, Art. no. 1376.
[8] K. Y. Yu, T. H. Yuen, S. S. M. Chow, S. Yiu, and L. C. K. Hui, "PE(AR)2: privacy-enhanced anonymous authentication with reputation and revocation," in *Proc. 17th Eur. Symp. Res. Comput. Security*, 2012, pp. 679–696.
[9] M. H. Au, A. Kapadia, and W. Susilo, "BLACR: TTP-free blacklistable anonymous credentials with reputation," in *Proc. 19th Annu. Netw. Distrib. Syst. Security Symp.*, 2012, pp. 1–17.
[10] J. K. Liu, M. H. Au, W. Susilo, and J. Zhou, "Linkable ring signature with unconditional anonymity," *IEEE Trans. Knowledge Data Eng.*, vol. 26, no. 1, pp. 157–165, Jan. 2014.
[11] S. Chen *et al.*, "Vehicle-to-everything (v2x) services supported by lte-based systems and 5g," *IEEE Commun. Standards Mag.*, vol. 1, no. 2, pp. 70–76, 2017.
[12] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: differential privacy for location-based systems," in *Proc. Conf. Comput. Commun. Security*, 2013, pp. 901–914.
[13] Tor Project, "Orbot: Proxy with tor," 2017. [Online]. Available: https://guardianproject.info/apps/orbot/. Accessed on: Aug. 15, 2017.
[14] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Proc. Adv. Cryptology*, 1986, pp. 186–194.
[15] B. Libert and D. Vergnaud, "Multi-use unidirectional proxy re-signatures," in *Proc. Conf. Comput. Commun. Security*, 2008, pp. 511–520.
[16] M. Z. Lee, A. M. Dunn, J. Katz, B. Waters, and E. Witchel, "Anon-pass: Practical anonymous subscriptions," *IEEE Security Privacy*, vol. 12, no. 3, pp. 20–27, May/Jun. 2014.
[17] C. Huang, R. Lu, H. Zhu, J. Shao, A. Alamer, and X. Lin, "EPPD: efficient and privacy-preserving proximity testing with differential privacy techniques," in *Proc. Int. Conf. Commun.*, 2016, pp. 1–6.
[18] M. H. Au, W. Susilo, and Y. Mu, "Constant-size dynamic k-taa," *IACR Cryptology ePrint Archive*, Rep. 2018/136, pp. 1–18, 2008.
[19] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," in *Proc. 24th Annu. Int. Cryptology Conf.*, 2004, pp. 56–72.
[20] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Proc. 24th Annu. Int. Cryptology Conf.*, 2004, pp. 41–55.
[21] S. Klemm *et al.*, "Autonomous multi-story navigation for valet parking," in *Proc. 19th IEEE Int. Conf. Intell. Transp. Syst.*, 2016, pp. 1126–1133.
[22] A. Ibisch *et al.*, "Towards autonomous driving in a parking garage: Vehicle localization and tracking using environment-embedded LIDAR sensors," in *Proc. IEEE Intell. Veh. Symp.*, 2013, pp. 829–834.
[23] M. Bertozzi, L. Castangia, S. Cattani, A. Prioletti, and P. Versari, "360 detection and tracking algorithm of both pedestrian and vehicle using fisheye images," in *Proc. Intell. Veh. Symp.*, 2015, pp. 132–137.

[24] D. González, J. Pérez, V. Milanés, and F. Nashashibi, "A review of motion planning techniques for automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 1135–1145, Apr. 2016.
[25] O. Blazy, G. Fuchsbauer, D. Pointcheval, and D. Vergnaud, "Short blind signatures," *J. Comput. Security*, vol. 21, no. 5, pp. 627–661, 2013.
[26] Y. Aikou, S. Sadiah, and T. Nakanishi, "An efficient blacklistable anonymous credentials without ttps using pairing-based accumulator," in *Proc. 31st IEEE Int. Conf. Adv. Inf. Netw. Appl.*, 2017, pp. 780–786.
[27] C. Garman, M. Green, and I. Miers, "Decentralized anonymous credentials," in *Proc. 21st Annu. Netw. Distrib. Syst. Security Symp.*, 2014, pp. 1–15.
[28] R. Yang, M. H. Au, Q. Xu, and Z. Yu, "Decentralized blacklistable anonymous credentials with reputation," *IACR Cryptology ePrint Archive*, Rep. 2017/389, pp. 1–36, 2017. [Online]. Available: https://eprint.iacr.org/2017/389
[29] J. K. Liu *et al.*, "Efficient privacy-preserving charging station reservation system for electric vehicles," *Comput. J.*, vol. 59, no. 7, pp. 1040–1053, 2016.
[30] R. Lu, X. Lin, H. Zhu, and X. Shen, "An intelligent secure and privacy-preserving parking scheme through vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 6, pp. 2772–2785, Jul. 2010.
[31] J. Ni, K. Zhang, X. Lin, Y. Yu, and X. Shen, "Cloud-based privacy-preserving parking navigation through vehicular communications," in *Proc. 12th Int. Conf. Security Privacy Commun. Netw.*, 2016, pp. 85–103.
[32] J. Ni, K. Zhang, Y. Yu, X. Lin, and X. Shen, "Privacy-preserving smart parking navigation supporting efficient driving guidance retrieval," *IEEE Trans. Vehicular Technol.*, vol. 67, no. 7, pp. 6504–6517, Jul. 2018.
[33] R. Garra, S. Martínez, and F. Sebé, "A privacy-preserving pay-by-phone parking system," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 5697–5706, Jul. 2017.
[34] L. Zhu, M. Li, Z. Zhang, and Z. Qin, "Asap: An anonymous smart-parking and payment scheme in vehicular networks," *IEEE Trans. Dependable Secure Comput.*, 2018. doi: 10.1109/TDSC.2018.2850780.
[35] Y. Luo, S. S. Cheung, R. Lazzeretti, T. Pignata, and M. Barni, "Anonymous subject identification and privacy information management in video surveillance," *Int. J. Inf. Security*, vol. 17, no. 3, pp. 261–278, 2018.
[36] A. Chattopadhyay and T. E. Boult, "Privacycam: A privacy preserving camera using uclinux on the blackfin DSP," in *Proc. IEEE Comput. Soc. Conf. Comput. Vision Pattern Recognit.*, 2007, pp. 1–8.
[37] T. Winkler and B. Rinner, "Security and privacy protection in visual sensor networks: A survey," *ACM Comput. Surveys*, vol. 47, no. 1, pp. 2:1–2:42, May 2014.



Cheng Huang (S'15) received the B.Eng. and M.Eng. degrees from Xidian University, Xi'an, China, in 2013 and 2016, respectively. He is currently working toward the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. He was a Project Officer with the INFINITUS Laboratory, School of Electrical and Electronic Engineering, Nanyang Technological University, till July 2016. His research interests include applied cryptography, cyber security, and privacy in the mobile network.

Rongxing Lu (S'09–M'10–SM'15) received the Ph.D. degree from the University of Waterloo, Waterloo, ON, Canada, in 2012. He has been an Assistant Professor with the Faculty of Computer Science, University of New Brunswick, Fredericton, NB, Canada, since August 2016. Before that, he was an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from April 2013 to August 2016. He was a Postdoctoral Fellow with the University of Waterloo from May 2012 to April 2013. His research interests include applied cryptography, privacy enhancing technologies, and IoT-Big Data security and privacy. He was awarded the most prestigious Governor General's Gold Medal, and has won the 8th IEEE Communications Society (ComSoc) Asia Pacific (AP) Outstanding Young Researcher Award, in 2013. He is presently a Senior Member of IEEE Communications Society. He is currently the Vice-Chair (Publication) of IEEE ComSoc CIS-TC.

Xiaodong Lin (M'09–SM'12–F'17) received the Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, Beijing, China, and the Ph.D. degree in electrical and computer engineering (with Outstanding Achievement in Graduate Studies Award) from the University of Waterloo, Waterloo, ON, Canada. He is currently an Associate Professor with the Department of Physics and Computer Science, Wilfrid Laurier University, Waterloo, ON, Canada. His research interests include wireless network security, applied cryptography, computer forensics, software security, and wireless networking and mobile computing.

Xuemin (Sherman) Shen (M'97–SM'02–F'09) received the Ph.D. degree in electrical engineering from Rutgers University, New Brunswick, NJ, USA, in 1990. He is currently a University Professor with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. His research focuses on resource management in interconnected wireless/wired networks, wireless network security, social networks, smart grid, and vehicular ad hoc and sensor networks.

Dr. Shen received the James Evans Avant Garde Award in 2018 from the IEEE Vehicular Technology Society, the Joseph LoCicero Award in 2015, and the Education Award in 2017 from the IEEE Communications Society. He has also received the Excellent Graduate Supervision Award in 2006 and the Outstanding Performance Award in 2004, 2007, 2010, and 2014 from the University of Waterloo and the Premiers Research Excellence Award in 2003 from the Province of Ontario, Canada. He was the Technical Program Committee Chair/Co-Chair for the IEEE Globecom'16, the IEEE Infocom'14, the IEEE VTC'10 Fall, the IEEE Globecom'07, the Symposia Chair for the IEEE ICC'10, the Tutorial Chair for the IEEE VTC'11 Spring, the Chair for the IEEE Communications Society Technical Committee on Wireless Communications, and P2P Communications and Networking. He is the Editor-in-Chief of the IEEE INTERNET OF THINGS JOURNAL and the Vice President on Publications of the IEEE Communications Society. He is a registered Professional Engineer of Ontario, Canada, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, and a Distinguished Lecturer of the IEEE Vehicular Technology Society and Communications Society.