Privacy-preserving solution for vehicle parking services complying with EU legislation

Petr Dzurenda, Florian Jacques, Manon Knockaert, Maryline Laurent, Lukas Malina, Raimundas Matulevicius, Qiang Tang, Aimilia Tasidou

Privacy-Preserving Solution for Vehicle Parking Services Complying with EU Legislation

Petr Dzurenda (1) Florian Jacques (2)
Manon Knockaert (2) Maryline Laurent (3)
Lukas Malina (4) Raimundas Matulevičius (5)
Qiang Tang (6) Aimilia Tasidou (3) *

December 2022

Abstract

Nowadays, a lot of modern cities adopt online smart parking services as best practices. Citizens can easily access these services using their smartphones or the infotainment panels in their cars. These services' primary objective is to give drivers the ability to quickly identify free parking slots, which should reduce parking time, save fuel, and relieve traffic in urban areas. However, the privacy offered by these services should be comparable to that of the standard paper-based parking solutions offered by parking ticket machines. On the other hand, a privacy-preserving smart parking service's design may raise a number of issues, including how to prevent double or multiple uses of parking tickets, how to prevent user tracking and profiling, how to revoke malicious users, how to handle data statistics without violating users' privacy, and how to comply with regulations like the General Data Protection Regulation (GDPR). In this article, we present multidisciplinary research on a comprehensive vehicle parking system that protects users' privacy. The research includes a range of topics, from the examination of regulatory compliance to the design of privacy-preserving parking registration and vehicle parking services to the implementation of privacy-preserving parking data processing features for data analysts. We provide a security analysis of our concept as well as several experimental results.

*(1) Department of Telecommunications, Brno University of Technology, 61600 Brno, Czech Republic - (2) University of Namur, Belgium - (3) TELECOM SudParis, Samovar lab, Institut Polytechnique de Paris, 91011 Paris, France - (4) Department of Telecommunications, Brno University of Technology, 61600 Brno, Czech Republic - (5) Institute of Computer Science, University of Tartu, 51009 Tartu, Estonia - (6) IT for Innovative Services (ITIS) Department, Luxembourg Institute of Science and Technology (LIST), 4362 Luxembourg, Luxembourg

Introduction

In future smart cities, smart parking solutions will be more and more integrated with city services and used by numerous citizens via their smartphones or infotainment panels in their vehicles. The main goal of smart parking services is to provide drivers the efficient detection of vacant slots that should shorten the time during parking, save fuel and decrease congestion in cities. Parking in city streets and parking lots is usually for specific fees according to different zones, periods, and daily times. Therefore, parking services usually have to collect these fees from users. Using parking lot terminals with tollgates should help with a payment collection, and only users who paid for the service should get access to the parking lots. Nevertheless, using prepayment and intelligent detection of free slots via mobile applications causes that users have to interact remotely with a smart parking system in advance. These systems should ideally provide a similar level of privacy as the traditional paper-based parking solutions with parking ticket machines. The design of a privacy-preserving smart parking service may open several issues such as how to prevent double/multiple spending of parking tickets, how to prevent user tracking and linking, how to revoke malicious users, how to handle data statistics without privacy breaches and how to be compliant with regulations such as General Data Protection Regulation (GDPR).

In this paper, we proposed a novel privacy-preserving solution for vehicle parking services which is complying with European Union (EU) legislation, especially with privacy and security requirements defined by current regulations and directives. The system protects users' privacy and their digital identities. Furthermore, it also allows third parties such as research institutions to run statistical analyses on parking data. This analysis can be done without impacting the privacy of both, i.e. users (no personal data or linkable information about users are disclosed) and analysts (no information about what they are searching for is revealed). To do so, we had to answer three main Research Questions (RQ):

- **RQ1:** What are the legal instruments, issues, and requirements for the deployment of such a system?
- **RQ2:** How to build a privacy-preserving system which meets the requirements from RQ1? Which Privacy-Enhancing Technology (PET) can be used in order to protect users' privacy during using the system, i.e., reservation of parking slots and parking vehicle actions?
- **RQ3:** How to allow third parties to perform statistical analyses on the parking transaction data, in a privacy preserving way? Which PET can be used to support this task?

The paper is organized as follows. Section 1 analyzes the recent research on security and privacy in smart cities with a focus on parking service applications. Section 2 introduces a high-level architecture description of our parking

system, security and privacy requirements. Section 3 presents the different legal instruments relevant for the deployment of vehicle parking systems. Section 4 outlines the used notation needed to understand the cryptographic design of our parking system. Section 5 introduces our privacy-preserving parking system, its security analysis, and experiment results. Section 6 presents our solution for privacy-preserving parking data processing, its security analysis, and experimental results. In Section 7, we conclude this work.

1 Related Work

In many existing works, smart parking services are usually considered as the part of smart cities or intelligent infrastructures. There are several works that deal with general security and privacy issues in smart cities and deal partially with parking services, such as [49, 60, 61, 50]. Further, privacy-preserving smart parking solutions and parking related problems in cities have been introduced in recent works such as [36], [16], [40], [67], [11], [2], [33], [21] and [44].

For example, [36] proposed a practical privacy-preserving pay-by-phone parking system based on periodical e-coin micro-payments for short intervals. The proposal deploys Hash-Based Message Authentication Codes (HMAC), RSA signatures, Chaum's blinded signatures based on RSA introduced in [17] and ECDSA signatures. The drawback of the proposal can be technical issues such as lack of coverage, low battery, etc.

In [11], the authors claimed that it has solved these technical disadvantages in their proposal of a privacy-preserving pay-by-mobile parking system. Their e-coin based proposal offered the same privacy as the traditional paper-based approach. Users' privacy is preserved without requiring a trusted party. The proposal deploys the Chaum's blinded signatures based on RSA and DSA. Later, [10] presented an upgraded and more efficient solution than in [11]. Nevertheless, both solutions digitally collect also car plate numbers (licenses) by parking officers.

[16] investigated privacy-preserving smart parking systems using IoT platform. They adopted Elliptic Curve Cryptography (ECC) as an attractive alternative to RSA-based solutions. They showed how to deploy zero-knowledge proofs (ZKP) using ECC that should preserve users' privacy. Moreover, they created a real-world outdoor IoT testbed and analyzed the execution time on various IoT platforms. Their work did not provide a tailored proposal but offered interesting practical results.

[40] presented a secure and privacy-preserving reservation/parking solution for automated valet parking systems without a trusted third party. Their solution is based on zero-knowledge proofs proposed by [34], geo-indistinguishable mechanism published in [3], proxy re-signatures designed by [47], and bloom filter data structure. Their parking reservation costs almost 3 seconds due to deploying the heavy cryptographic operations. [67] focused on smart parking in cities and presented the anonymous smart-parking and payment scheme in vehicular networks. Their solution is based on the Pointcheval-Sanders random-

izable signature designed by [54] and using a trusted authority. For generating a parking query, one driver has to compute several exponentiations, multiplications, additions, and hash.

[2] presented a privacy-preserving smart parking system using blockchain and private information retrieval. A shared ledger should increase security, transparency, and availability. The system preserves drivers' location privacy by using the private information retrieval of parking offers from the blockchain nodes and deploying short randomizable signatures proposed in [54] allow drivers to anonymously reserve available parking slots. The reservation time is around 1 ms at 1.2 GHz Processor with 160-bits MNT curve and SHA-2. Similarly, [33] presented a blockchain-based privacy-preserving valet parking protocol. The solution is based on a new variant of Pointcheval-Sanders group signature, and it is secure in the random oracle model. Blockchain-based privacy-preserving decentralized parking recommendation solutions has been also proposed by [46]. Their solution employs a private blockchain, a bulletin board, a re-randomized homomorphic encryption scheme, zero-knowledge protocols and oblivious pseudorandom functions. Recently, [21] have proposed the privacy-preserving online parking system based on blockchain and smart contracts. The system deploys provable secure cryptographic primitives such as revocable anonymous credential proposed in [39] and partially blinded signature proposed in [1]. The system provides a full set of privacy-enhancing features such as user anonymity, untraceability, and unlinkability. Furthermore, the authors involve blockchain and smart contracts technologies in the payment and verification phases to make the system more transparent, decentralized, and resistant against cyberattacks.

The complex taxonomy of smart parking and autonomous valet parking solutions has been presented in the recent survey by [44]. This survey studies many aspects of parking solutions, where security and data privacy processing have been detected as ones from challenges and future directions.

Few related works have also studied legal challenges and regulations in smart cities and parking services. For example, [66] provides a regulatory view on smart city services where smart parking systems are integrated, and [48] deals with legal challenges in smart cities. Nevertheless, a detailed study focusing on the regulation requirements of smart parking systems is still missing.

In this paper, we focus on a complex spectrum of problems in privacy-preserving smart parking including legal and technical perspectives in order to cover various layers (authentication, secure communication, data processing, and other aspects). Our multidisciplinary work presents a comprehensive privacy-preserving proposal for parking services that covers privacy-preserving parking requests, privacy-preserving data statistics, regulation compliance, and other privacy issues related to communication and system settings.

2 Parking Scenario Description

In this section, we present a high-level system architecture, and we define the system entities, the parking scenario phases, and the privacy and security re-

quirements.

2.1 System Architecture

Three types of entities interact in our privacy-preserving vehicle parking system:

- **Parking Service Provider** (PSP): The PSP generates cryptographic parameters and keys. It also registers new users and revokes/identifies the malicious ones. Furthermore, the PSP mediates communication between users and the PLT and enrolls new PLTs in the system. The communication with the PSP takes place fully via an Internet connection. We assume that the PSP is a semi-trusted party which honestly runs the algorithms but could be curious.
- **Parking Lot Terminal** (PLT): The PLT represents the system controlling access to the specific parking lot. It is responsible for issuing the parking permits to users and verifying the presented parking permits by users. The communication with the PSP takes place via an Internet connection during the parking permit issue phase (reservation parking in the parking lot) and via Bluetooth connection during the parking permit verification phase (accessing the parking lot).
- **User Device**: The user is represented by its device, typically a smartphone. These devices allow storing users' parking permits issued by the PLT through the PSP and presenting these permits to the PLT when users access the parking lot. Furthermore, this device holds system parameters, generates and stores user cryptographic keys, communicates with PSP via Internet connection (i.e., Wi-Fi, Long Term Evolution (LTE)) and with PLT via the Bluetooth Low Energy (BLE) interface.

The privacy-preserving parking system with all involved entities and protocols is depicted in Figure 1. The proposal also involves a trusted third party - IDentity Provider (IDP) that manages user identity and associated identity attributes.

2.2 Trust Assumptions

We assume that communication between all communication parties is secured. In particular, the communication between users and the PSP and the communication between the PSP and PLTs is secured by Transport Layer Security (TLS) protocol. The whole system is based on a trust chain, i.e., we expect the existence of Public Key Infrastructure (PKI) and trusted certification authorities. Besides the privacy-enhancing protocols used in our parking system in each scenario phase described in Section 5.1, we need to consider also other privacy issues which can impact users privacy:

- **Anonymous Payment Methods**: The payment to PLT can be done privately by deploying the improved e-payment 3D-Secure protocol [53] or

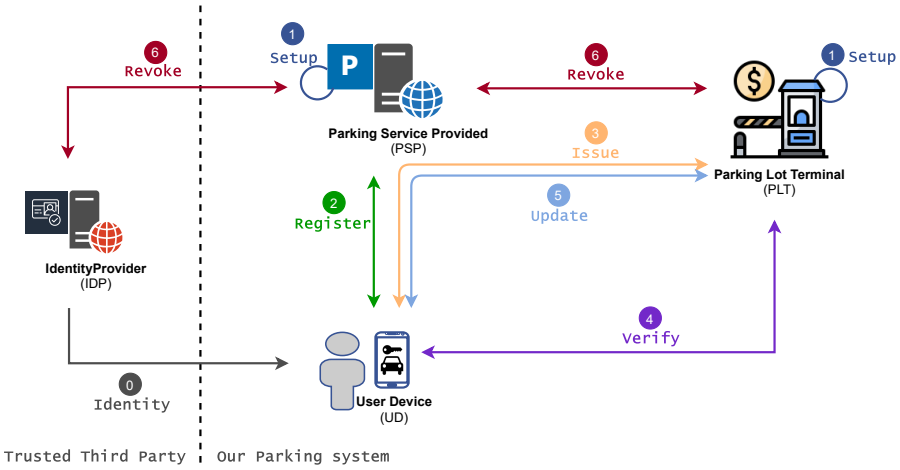

Figure 1: Privacy-preserving parking system.

by using popular wallets on mobile devices that support privacy-preserving cryptocurrencies, i.e., Monero [51], Zcash [43], and DASH [19]. The security and privacy of popular Android wallets have been studied in [7].

- **Anonymous Communications in Wide Area Network (WAN)**: Privacy-preserving communication in WAN can be achieved by mature onion routing protocols and techniques such as ToR [18]. Then, users are able to privately communicate with PSP via Internet during their registration and issuing parking permit. On one hand, users' source addresses and actual locations are hidden to PSP and observers because the ToR protocol applies at least 3 randomly-selected servers (onion routers) as relays and encrypts the communication (creating the onion layers). On the other hand, communication via ToR can cause delays due to encryption operations and using more hops.

- **Anonymous Communications in Personal Area Network (PAN)**: For PAN, one typical technology is Bluetooth Low Energy (BLE). By design, BLE provides a reasonable level of privacy protection with features like address randomization [15] and it has been widely used in contact tracing for COVID-19, e.g., [59]. Therefore, we can assume that BLE provides a sufficient level of anonymity/privacy guarantee in our application.

- **Surveillance Minimization**: Surveillance security systems with cameras are usually deployed in parking lots and garages in order to increase security against various physical attacks, vandalism, and thefts. Moreover, some solutions are based on using Automatic Number Plate Recognition (ANPR) or Licence Plate Recognition (LPR) to detect concrete vehicles that prepaid a service. Nevertheless, these camera systems could conflict

with users' privacy and GDPR. Thus, it is necessary to use records and basic functionality of ANPR only for security purposes and not to store records for longer periods or non-permitted tracking.

2.3 Scenario Phases

Our parking scenario consists of the following phases:

1. **Register user phase**: The digital identity of the user is created in this phase, as illustrated in Figure 2. First, the users download the mobile application of the parking system, e.g., using Google Play (see, *1.1. Download mobile parking application*). Second, the users use the application to create their own digital identity in the parking system. To do so, we suggest involving a trusted third party that will manage user identity and associated identity attributes (see, *1.2. Create digital identity (through trusted third party)*). This party is called IDentity Provider (IDP). Thanks to using the IDP, we do not need to store sensitive user data, such as name, surname, address, age, gender. Otherwise, these data can directly identify the user and can be a target of cyberattacks. Therefore, we suggest to deploy one from these following methods to create a digital identity in the parking system:

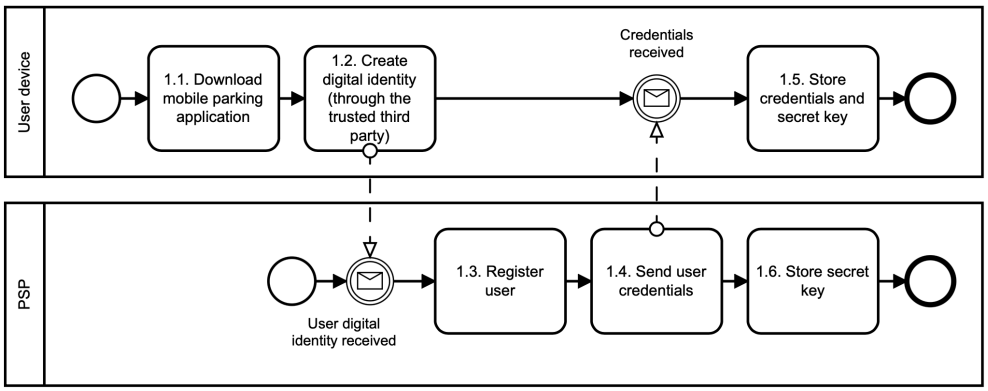

Figure 2: Register user.

- **Payment card binding**: The users have to add their bank cards to the parking application. The PSP does a pre-authorization charge to make sure the payment card used by the user is valid. If so, the PSP will create the digital identity of the user. The digital identity is represented by the payment card number provided by the user. The PSP learns no more information about the user. If the user commits fraud, the PSP will query disclosing the user identity to the bank that issued the payment card.

- **Mobile number binding**: The users have to add their phone number to the parking application. The PSP sends an authorization code to this phone number to make sure the phone number provided by the user is valid. If so, the PSP will create the digital identity of the user. The digital identity is represented by the phone number provided by the user. The PSP learns no more information about the user. If the user commits fraud, the PSP will query disclosing the user identity to the mobile operator. In this case, it is necessary to have a registered telephone number, such as in some European Union (EU) countries. For example, all SIM cards in Spain need to be registered by law.
- **Electronic identification (eID) binding**: The user has to use trusted Identity Provider (IDP) supported by the PSP and according to the EU electronic identification and trust services (eIDAS) Regulation. For example, in the Czech Republic, we can find the eObčanka application. The PSP learns no more information about the user. If the user commits fraud, the PSP will query disclosing the user identity to the organization delivering public digital services in an EU member state.

When the digital identity of the user is created, the PSP runs the `Register` algorithm (see, *1.3. Register user*). In particular, the PSP generates the user access credential Λ and user secret key sk_U. To do so, the PSP will use group signature [38]. The credential and the secret key are sent to the user's device (see, *1.4.Send user credentials*) where they are securely stored (see, *1.5. Store credentials and secret key*). Furthermore, the secret key is also stored in the PSP Revocation Database (RD) (see, *1.6. Store secret key*). The PSP can use this database to revoke or identify malicious users. The user revocation is possible only in collaboration with the PLT. The user identification requires also the involvement of IDP.

2. **Issue parking permit phase**: The parking reservation is made through the PSP. The PSP acts as a gateway between the user and the PLT, as illustrated in Figure 3. The PSP does not interfere with the `Issue` algorithm. It only forwards the communication between communicating parties. The `Issue` algorithm is run between the user device and the PLT. First, the user sends a parking request to the PLT (see, *2.1. Send parking request*). Basically, this information is where, when, and for how long the user wants to park. No sensitive, personal, or other *linkable* data are provided. This information is sent in a clear way, and therefore both the PSP and the PLT know them. Furthermore, the reservation request also includes the user access credential Λ issued by the PSP. This credential is blinded, and therefore, the PSP nor PLT can learn it in this phase. Additionally, the access credential Λ is randomized with a session credential key sk_{Cred}. This key is generated by the user for each new reservation phase, and therefore, it differs for all user's parking permits. Second, af-

ter the payment for the parking is done (see, *2.3. Perform payment*), the PLT generates parking permit ID (see, *2.5. Generate parking permit*) and computes a partially blind signature [1] on parking request data (both, clear and blind information) and sends it to the user (see, *2.6. Send parking permit*). The user uses the partially blind signature from the PLT to reconstruct the parking permit $CRED$. The PSP and the PLT do not see the whole parking permit. They see only its public data, i.e. parking permit ID (`PPID`), parking location (`PLTid`), parking time (`time_duration`) and information about parking time extension (`EPT`).

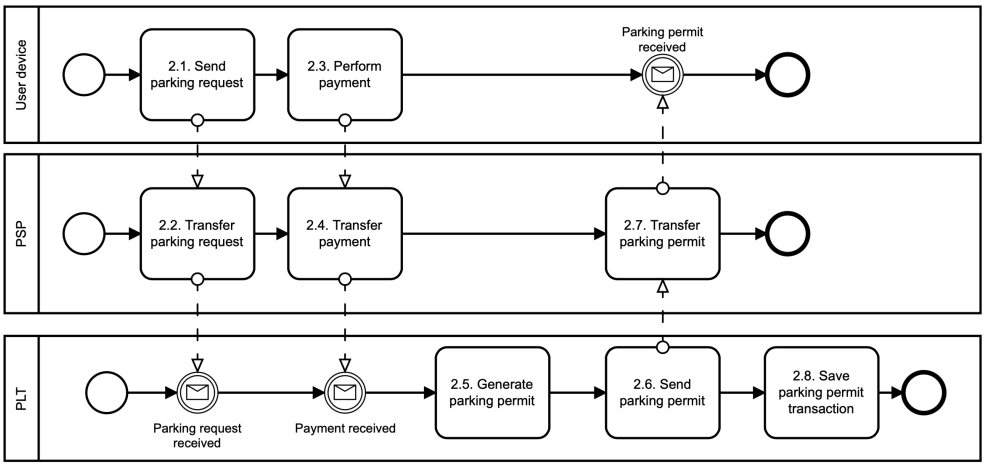

Figure 3: Issue parking permit.

3. **Park vehicle phase**: The user accesses the parking lot in this phase as illustrated in Figure 4. To get access, the user must authenticate to the PLT first (see, *3.1. Authenticate* and *3.2. Confirm*). During the parking vehicle phase, the user communicates directly with the PLT, for example, via a Bluetooth communication interface. First, the user sends the parking permit to the PLT (see, *3.3. Send parking permit*). The PLT checks the parking permit data and verifies the signature on the permit using PLT's public key pk_{PLT} (see, *3.4. Verify signature*). If the parking permit is valid, the users must prove that the parking permit belongs to them (see, *3.5. Check user authentication proof*), i.e., the permit includes the access credential Λ issued by the PSP and randomized by the user with the credential key sk_{Cred}. To do so, the user and the PLT run the `Verify` algorithm. The PLT checks the user's authentication proof using PSP's public key pk_{PSP}. If the proof is valid, the user is allowed to access the parking lot and the barrier is opened (see, *3.6. Allow vehicle to enter* and *Enter PLT and park vehicle*). The parking permit includes user access credential Λ which can be used for linking the parking permit to the real identity of the user. However, this access credential is randomized with

different credential keys in all issued user's parking permits. Therefore, the PLT cannot link two different parking permits to the one user, and therefore, the user access parking lot *anonymously* and *unlinkably*. This prevents the possibility of profiling and tracking users across the system. The PLT is not able to get any information on how often users park their vehicles in the parking lot.

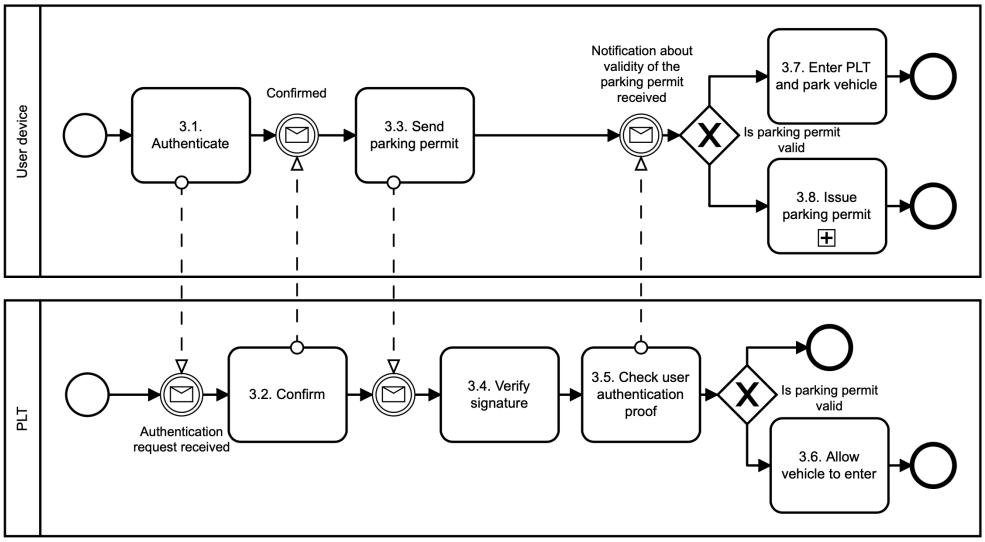

Figure 4: Park vehicle.

4. **Extend parking time phase**: The users can extend their parking time period using the `Update` algorithm as illustrated in Figure 5. Users do not need to reveal any personal data to extend the parking time. The main assumption is that the PLT already has the user's parking permit, i.e., the user parked the vehicle in the parking lot. First, the user sends the extension parking time request to the PSP (see, *4.1. Send the extension parking time request*). This request includes `PPID` and `PLTid` information. Thanks to `PLTid` the PSP finds the relevant PLT (see, 4.2 *Transfer the extension parking time request*). Because of the `PPID`, the PLT finds the relevant parking permit (see, 4.3 *Find relevant parking permit*). If the extension parking time is possible (see, *4.4. Check if extension is possible*), then the user and the PLT run the `Verify` algorithm in order to authenticate and authorize the user. If the user is authenticated, then the user and the PLT run the `Issue` algorithm with a new extended time period (see, *4.7. Issue parking permit* and Figure 3). The `Issue` algorithm is run after the payment for the extended parking time is made.

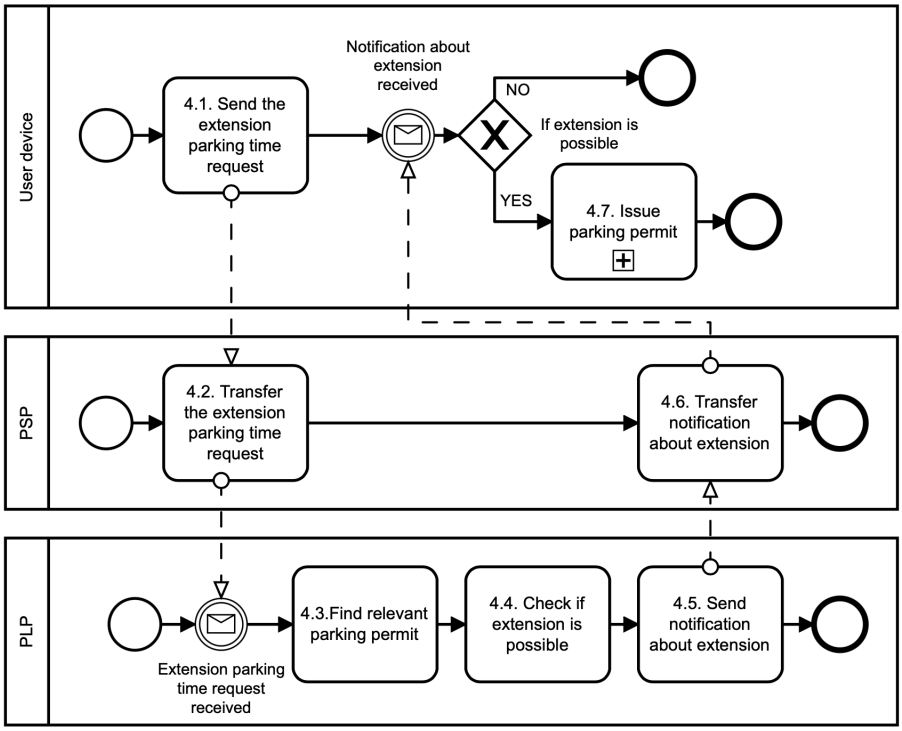

Figure 5: Extend parking time.

2.4 Privacy and Security Requirements

This section introduces general security and privacy requirements on the parking reservation system. In particular, we have the following system security requirements:

- **Authentication**: Parking permits from PSP should be granted only to valid non-revoked users who use them in the parking phase. The users should stay in anonymity but should prove that they hold valid parking permits (based on reservation) to PLT when the user arrives at a parking lot.
- **Data confidentiality**: All sensitive and personal data, e.g., Vehicle Plate Number (VPN) or vehicle IDs, should be secured. Data eavesdropping and exposure should be prevented by data encryption. The system should not reveal any sensitive personal data during issuing the parking permit and the park vehicle phase.
- **Data authenticity and integrity**: All exchanged data (e.g., parking permits, information about available slots, notifications) should be secured against their tampering by unauthorized parties.

Furthermore, we identify the following system privacy requirements:

- **Data privacy**: All stored and exchanged data should not be exposed to undesired parties and eavesdroppers, e.g., user's vehicle ID, user parking history, and user profiles.
- **Pseudonymity**: A user should be pseudonymous and should be identifiable only in case of certain conditions by PSP. Users should not be identifiable while using the parking system by external and internal parties (PLTs) or other users.
- **Unlinkability**: PSP, PLTs, and other users should not be able to link together the parking actions of the same user (vehicle). The system should not scan VPNs.
- **Conditional traceability**: PSP should not be able to trace users' credentials and their parking actions if the users are honest. PSP should be able to open a user's identity from the parking permit only in case of serious fraud and by cooperation with PLT.
- **Revocation**: PSP should be able to conditionally open the parking permit credentials and identify the user. In a serious incident, PSP can remove a user from the system or remove the user's anonymity. To do so, PSP should collaborate with PLT or, where appropriate, with other trusted third parties.

For data processing, it is necessary that the parking transaction records produced during the system use are stored and processed in a privacy-preserving manner at the PSP under the control of the PLT, thus leading to the following additional security and privacy requirements:

- **Data minimisation**: The transaction data items stored should be reduced only to the necessary data items for service usage analysis.
- **Index and document privacy**: The encrypted data used for statistics extraction should not reveal any sensitive information about the plaintext data and keywords (used for statistics purpose), to any unauthorized entities including the storing PSP.
- **Query privacy**: The type of statistics being performed should remain confidential, to the storing PSP.
- **Access pattern privacy**: No additional information should be revealed from the search results about the data involved.
- **Query authorization**: Statistics extraction should be limited to authorized entities and authorized keywords only.

3 Legal Issues

The objective of this section is to present the different legal instruments relevant for the deployment of such a service in order to answer the first research question, i.e., **RQ1:** What are the legal instruments, issues, and requirements for the deployment of such a system? After an explanation of the legal framework surrounding user identification[1], the second section focuses on the security requirements in the scenario presented. The legal instruments studied relate to (i) use and deployment of Intelligent Transport Systems (ITS) [29] (ii) consumer protection [30], [28], and (iii) safety requirement for market placement of vehicles and their components [32], [63].

3.1 Smart parking scenario and data protection requirements

The GDPR applies to any processing of personal data [31], Art. 4. In its guidelines on connected vehicles, the European Data Protection Board (EDPB) states that: "Even if data collected by a connected car are not directly linked to a name, but to technical aspects and features of the vehicle, it will concern the driver or the passengers of the car" [23], page 5. Under GDPR, personal data is therefore a broad notion [55]. Thus, in the scenario studied, there will be different ways of identifying data subjects, in particular through vehicle identification and payment service. Hence, use of such information fall under the material scope of GDPR.

In the scenario studied, additionally to the requirements of lawfulness [31] Art. 5, of transparency [31] Art. 12, of data accuracy [31] Art. 5.1, d) and the data storage limitation [31] Art. 5.1, e) [45][2], a fundamental question is the appropriateness of identifying the service user. Indeed, the EU places at the heart of personal data protection the principle of protection by default and by design [31] Art. 25[3]. To be compliant, one prior question is the need for user identification [31] Art. 5.1, c). This implies determining, at each stage of the development of the service and according to the activities of the PSP and

[1]The reader should bear in mind that the following lines are not intended to provide a detailed analysis of the application of the EU General Data protection Regulation (GDPR) in the scenario presented.; Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 27 April 2016, OJ L119/1. Far from being exhaustive, we draw attention to the existence of EDPB guidelines on connected vehicles [24]. In this paper, we will not focus on the Directive 2009/136 and the E-privacy proposal. It should be noted that a connected vehicle might be interpreted as a terminal equipment under the EDPB guidelines on connected vehicles (Guidelines 01/2020). This means that the E-privacy Proposal could then be applied when it is necessary to access the information stored in the vehicle (e.g. when presenting the parking permit to the Parking Lot Terminal (PLT). Moreover, depending on the purpose, consent may or may not be required in the sense of the E-privacy proposal

[2]Art. 29 Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things, 16.09.2017, WP 223.

[3]EDPB, Guidelines 04/2019 on Article 25- Data Protection by Design and by Default, 20 October 2020, [25]

PLT, whether it is necessary to identify the person. Even if an identification is possible by the PSP with personal information such as mobile phone number, bank card and the credential, the minimisation principle is facilitated by the use of a third party, such as IDentity Provider (IDP), to avoid the collection of unnecessary personal data by the PSP. Additionally, each entity (IDP, PSP, and PLT) has no access to the same personal data.

Secondly, if identification is necessary, each entity responsible for the processing must favour the use of pseudonymisation [31] (Art. 4.5) techniques. Indeed, the user is identified only in some situations by the PSP and the pseudonymisation is favoured for the PLT. The same credential than the one created by the PSP is pseudonymised for the PLT because these privacy-enhancing technique is sufficient to fulfil its purpose. The pseudonymisation is reinforced by unlikability parameters (PSP, PLTs or other users should not be able to link together parking actions of the same user if the parking permit is not recorded for a long period of time by the PLT (principle of storage limitation contained in Art. 5 [31]). Finally, it is important to stress that the principle of minimisation is not only about the need or not to identify the data subject, but also about the need to determine an access policy to the personal data processed. Article 25.2 of the GDPR specifies that the control of accessibility to personal data is an integral part of the default data protection principle and states that: "In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons". In this respect, the parking space reservation service and the payment service should be able to log who accessed to the data subject's data and the possibility to determine whether they have consulted or modified the information are two security measures that should be implemented [20][4].

The EDPB states that: "the plurality of functionalities, services and interfaces (e.g., web, USB, RFID, Wi-Fi) offered by connected vehicles increases the attack surface and thus the number of potential vulnerabilities through which personal data could be compromised ($\cdots$) In addition, personal data stored on vehicles and/or at external locations (e.g., in cloud computing infrastructures) may not be adequately secured against unauthorized access" [23], pages 11-12[5]. According to article 32 of the GDPR, data controllers and data processors have to implement appropriate technical and organizational measures to ensure security of personal data, considering the state of the art, the costs of implementation, the type of personal data, and the potential risks. Several security measures are planned, notably for the communication between users and the PSP and the communication between the PSP and the PLT (see also Section 2.3 concerning the architecture and the protocols used and Section 5 regarding the cryptographic design). In particular, the cryptography and the

[4]EDPB, Guidelines 04/2019 on Article 25- Data Protection by Design and by Default, 20 October 2020, p.13 stating that "Access controls should be observed for the whole data flow during the processing". In the smart parking scenario, see for example the rules of access between the PSP and the PLT

[5]ENISA, Cyber Security and Resilience of smart cars, December 2016, p.34 highlighting that in general, "the attack surface of a smart car is very large".

pseudonymization technologies are cited by the GDPR as security measures making identification of data subjects more complex.

3.2 Additional privacy and security requirements

3.2.1 Deployment and use of intelligent transport systems

In Directive 2010/1024 on the framework for the deployment of ITS in the field of road transport, ITS are defined as "systems in which information and communication technologies are applied in the field of road transport $(\cdots)$ and in traffic management and mobility management $(\cdots)$" [29], Art. 4.4. The provision of services for (i) information on parking places and (ii) reservation of parking places for trucks and commercial vehicles are two priority actions for the Directive [29], Art. 3. Thus, if the smart parking service also targets commercial vehicles, the PSP might be qualified as provider of an ITS service for reservation of parking places. PSP and/or PLT may also be considered as providers of an ITS information service on parking places. Information on availability may indeed constitutes a preliminary step for reservation of a parking place.

ITS directive contains specific privacy and security requirements where personal data are processed for the operation of an ITS application or service [29], Art. 10. First, data processing must be pursued in compliance with the GDPR. Second, personal data can be processed only where necessary for the performance of the application/service. Use of anonymous data is strongly suggested. Third, integrity and confidentiality of the data must be ensured. As explained above, personal data is indeed processed. Nevertheless, the data seems necessary in relation to the provided service and in accordance with a data minimization perspective.

3.2.2 Consumer protection rules

The definition of user used for the smart parking scenario is sufficiently broad to include consumer protection law. Indeed, consumer protection rules may apply if the user of the smart parking service is a natural person acting outside its professional activity (i.e., in Business-to-Consumer (B2C) relationships). In this context are especially relevant, (i) the Directive 2019/770 on contracts for supply of digital contents and services and (ii) the Directive 2019/771 on sale contracts of goods. The first Directive applies to conformity assessment of digital contents/services while the second applies to conformity assessment of good incorporating or interconnected with digital contents/services [28] [57]. Directive 2019/771 also applies to digital content or services incorporated or interconnected to goods – and which are essential for the performance of the goods – provided under the sale contract of these goods.

In the case at hand, due to the two possibilities for users to interact with the parking system, both Directives may apply depending on the means used in order to initiate the parking permit request. When the reservation process is enabled with a standalone application available on the user's mobile phone,

the PSP who serves as a software interface between the user and the PLT could be qualified as digital content or service provider under Directive 2019/770 [30], recital 19. On the contrary, if the parking permit request process is triggered by a dedicated on-board unit, this device will meet the definition of good with digital elements according to Directive 2019/771 [14]. Both Directives highlight importance of security updates and requires that such updates are provided to the consumer in order to keep the good or digital contents/services conform [30] Art. 8., [28] Art. 7.3, [5]. Both provisions highlight that provider of digital contents/services or sellers of goods will not be liable for lack of conformity if the consumer chooses not to install update, only if they have been informed of the importance of the updates to maintain conformity.

3.2.3 Vehicle safety requirements

In order to obtain EU type approval (i.e. homologation), manufacturers of vehicles, vehicles systems and components must comply with Regulation 2019/2144 (hereafter the "Vehicles General Safety Regulation"), [4]. Manufacturers must demonstrate compliance with several technical regulations adopted by the EU or the United Nations Economic Commission for Europe (UNECE), including on protection against cyberattacks [32] Art 4.5 d. Even if the vehicles general safety Regulation applies primarily to vehicles manufacturer, it may still apply to the scenario studied depending on choices made for the specific architecture of the parking permit request process and the means used to initiate this process (e.g. if the reservation process is made through an on-board unit developed partly or wholly by the vehicle manufacturer).

Focus on UNECE Regulation n155 on vehicles cybersecurity: Through homologation, EU law imposes compliance with UNECE Regulation n 155 [22], which aims to ensure protection of vehicles and their functions against cyber threats to their electrical and electronical components (see Art. 2.2). This text requires that vehicles manufacturers have a CyberSecurity Management System (CSMS). This CSMS must go through a certification process and applies to the entire lifecycle of the vehicle types for which homologation is sought. Under this Regulation the notion of "Vehicle Type" designates vehicles that do not present differences for essential features of their electrical/electronical and external interface architecture. To this end, the Regulation contains requirements concerning the CSMS in general (i.e. independently from of the manufacturers' vehicles types) and requirements directed toward each vehicle type [37] (also see Articles 7.3 to 7.3.6 of UNECE Regulation for the requirements directed toward vehicle types). Only requirements relating to the CSMS of the manufacturer are presented below. Nevertheless, we highlight that, this Regulation imposes application of a risk identification process for each vehicle type. To that extent, critical elements of vehicles such as the one ensuring connectivity and the parts of the architecture enabling data exchange must be identified [62]. The following lines explain the potential application of this Regulation within the context of this paper.

Cybersecurity management system requirements: In order to certify a CSMS, the approval authorities must verify that different processes are implemented by the vehicle manufacturer [62] Art. 7.2 and 7.3. In order to identify the risks, threats and vulnerability to which vehicles of the manufacturer are exposed. An annex to the Regulation identifies high level threats/vulnerabilities and sub level threats/vulnerabilities (e.g. loss of data within cloud infrastructure, loss of data confidentiality/integrity) that must be covered by the CSMS. As specified by UNECE, risks linked to use of connected services are especially relevant in the process. Another requirement is the implementation of procedures to verify proper management of identified risks. To comply with this requirement, a list of mitigation measures, annexed to the Regulation, that include, among others, use of access control to personal data. Additionally, vehicle manufacturers must demonstrate to certification authorities, how the CSMS handles the dependencies and risks stemming from its supply chain[6].

Application of UNECE Regulation n155 to the smart parking service: Regarding the application of this Regulation in the context of this paper, different scenarios must be distinguished. First, the parking permit request process can be initiated by the user with an on-board unit integrated in the vehicle and developed by the vehicle manufacturer, i.e., the Original Equipment Manufacturer (OEM). Hence, this unit, as part of the vehicle, will be taken into account by the manufacturer within the assessment for compliance with the UNECE Regulation. Second, the on-board unit used to initiate the parking permit request might be developed by another entity (e.g. a tier one or tier two supplier) and integrated in the vehicle by the OEM. In this second scenario, the Regulation will create requirements for the OEM (e.g. assessing if the unit is a critical element of the vehicle). It will also apply to the supplier of the device which needs to cooperate with the manufacturer to handle supply chain related cyber risks (e.g., see ([64], [65], [8]). Third, the parking permit request may be enabled with a digital application developed by a third party (e.g. the PSP) in association with the vehicle OEM. This scenario raises the question of the qualification of the PSP in relation to the OEM's supply chain. In this context the European Union Agency for Cybersecurity (ENISA) considers that a software provider can be considered as a tier one provider when having direct contractual relationship with the OEM [26]. Thus, if the digital application is developed in collaboration between the OEM and the application provider, the Regulation requirements linked to management of the supply chain related to cyber risks may apply. Consequently, where a relation exists between the OEM

[6]To comply with this requirement, vehicle manufacturers have to demonstrate the possibility to identify and manage cyber risks linked to their supply chains. This means, among others, being able to (i) identify risks associated to components or services of suppliers and (ii) manage the risks associated to providers of connected services on which vehicles may rely. To that extent, UNECE considers this requirement as implying implementation of information sharing process on cyber risks with suppliers and joint process of incident management. Use of contractual agreement defining cyber security requirements is heavily recommended. Hence, this requirement produces effects on suppliers as it creates a duty to collaborate with the vehicle manufacturers [62]

and the service provider (through the on-board unit or an application), the PSP shall be able to demonstrate that its security measures (e.g., Section 5) allow for the OEM to comply with the requirements mentioned above.

In a last scenario the mobile application used for the permit request process may be developed by the PSP or a third party at the demand of the PSP without involvement of the OEM. In absence of contractual agreement with the application provider, the application offered to the user might fall outside the scope of UNECE Regulation [27]. However, according to ENISA "the UNECE Regulation $(\cdots)$ applies to all Connected and automated mobility stakeholders (including Operators of Intelligent Transport System) who must ensure that their products and services conform to cybersecurity goal" [27]. As stated above, the PSP may indeed be qualified of provider of an ITS.

As a preliminary conclusion and first response to RQ1, Table 1 identifies the legal instruments applicable to the scenario and the main data protection and security requirements to build a privacy-preserving system.

4 Cryptographic Preliminaries

We first outline the used notation needed to understand the cryptographic core of our privacy-preserving parking system. Then, we briefly introduce bilinear pairing maps and weak Boneh-Boyen (wBB) signature [9] which are used throughout all our cryptographic design. Finally, we review the protocols on which our scheme is based, namely a short group signature (HDMR18) proposed by [38], partially blind WI-Schnorr signature proposed by [1], and searchable symmetric encryption scheme proposed by [35].

From now on, the symbol ":" means "such that", "$|x|$" is the bitlength of x and "$||$" denotes the concatenation of two binary strings. We write $a \in_R A$ when a is sampled uniformly at random from A. A secure hash function is denoted as $\mathcal{H} : \{0,1\}^* \rightarrow \{0,1\}^\kappa$, where κ is a security parameter. We describe the Proof of Knowledge (PK) and the Signature of Knowledge (SK) protocols using the notation introduced by [13] (CS). In particular, the protocol for proving the knowledge of discrete logarithm of c with respect to g is denoted as $PK\{\alpha : c = g^\alpha\}$ and the protocol for proving the knowledge of discrete logarithm of c with respect to g and message m is denoted as $SK\{\alpha : c = g^\alpha\}(m)$.

4.1 Bilinear Pairing

Let G_1, G_2, and G_T be cyclic groups of the same prime order n, $p \in G_1$, $q \in G_2$, and $\mathcal{O}$ is the point at infinity. G_1 and G_2 are additive groups and G_T is a multiplicative group. By definition $(q, G_1, G_2, G_T, \mathbf{e}, g_1, g_2)$ is a bilinear group if it satisfies all below properties:

- **Bilinearity**: $\forall x, y \in Z_n, p \in G_1, q \in G_2 : \mathbf{e}(p^x, q^y) = \mathbf{e}(p, q)^{xy}$.

Table 1: Smart parking: Privacy and security requirements.

GDPR, [31]	ITS directive, [29]	Consumer protection (directives 2019/770 and 2019/771), [30], [28]	Vehicle safety regulation (UNECE regulation No 155), [32], [63]
Data minimization	Data minimization	Provision of security updates	Adoption of Cybersecurity management system and implementation within the organization
Pseudonymisation and encryption	Data anonymisation	Information on security updates availability and importance to maintain conformity of goods, contents or services.	Process for identification of risks, threats and vulnerabilities
Access control	Data integrity and confidentiality		Requirement to classify risks, assess risks probability and identify treatment measures (including impact assessment)
Data storage	User choice where sensitive personal data are processed (consent requirement)		Application of mitigation measures (list of mandatory measures annexed)
Secure contractually and technically the transfer of personal data			Effectivity test during design and production phases
Risk assessment and appropriate level of security			Continuous update of the risk assessment
			Processes to detect and react timely and appropriately to attacks/threats /vulnerabilities
			Forensic data collection requirement
			Management of supply chain related risks through contractual agreements, information sharing processes and joint incident management
			Identification of critical elements of vehicles

- **Non-degeneracy**: $\forall p \neq \mathcal{O}\ \exists q \in G_2 : e(p,q) \neq 1 \in G_T$ and $\forall q \neq \mathcal{O}\ \exists p \in G_1 : e(p,q) \neq 1 \in G_T$.
- **Computability**: There exists an efficient algorithm $\mathcal{G}(1^\kappa)$ to compute $\mathbf{e}(p,q)$.

In this work, we consider the case $G_1 \neq G_2$ that is when $\mathbf{e}$ is an asymmetric bilinear map and the Decisional Diffie–Hellman (DDH) assumption holds.

4.2 Weak Boneh-Boyen Signature

The Weak Boneh-Boyen (wBB) signature scheme is a pairing-based short signature scheme. The scheme is provably secure and it is proven to be existentially unforgeable against a weak (non-adaptive) chosen message attack [9]. The scheme can be easily combined with the zero-knowledge proofs as shown in [12]. This makes it possible to prove the authorship of signed messages in an unlinkable and anonymous manner. Below is a brief illustration of the wBB signature [9]:

- $(pk, sk, syspar) \leftarrow \texttt{KeyGen} \leftarrow (1^\kappa)$: On the input of the security parameter κ, the algorithm generates system parameters $syspar = (q, G_1, G_2, G_T, \mathbf{e}, g_1 \in G_1, g_2 \in G_2)$, computes $pk = g_2^{sk}$, where $sk \in_R Z_q$, and outputs sk as the private key and $(pk, syspar)$ as the public key.
- $(\sigma) \leftarrow \texttt{Sign} \leftarrow (m, syspar, sk)$: On the input of the message $m \in Z_q$, the system parameters $syspar$ and the secret key sk, the algorithm outputs the signature of the message $\sigma = g_1^{\frac{1}{sk+m}}$.
- $(1/0) \leftarrow \texttt{Verify} \leftarrow (\sigma, m, pk, syspar)$: On the input of the system parameters $syspar$, the public key pk, a signature σ and a message m, the algorithm returns 1 if and only if $\mathbf{e}(\sigma, pk) \cdot \mathbf{e}(\sigma^m, g_2) = \mathbf{e}(g_1, g_2)$ holds, i.e. the signature is valid, or 0, otherwise.

4.3 Short Group Signature HDMR18

The article [38] presents a short and fast group signature scheme (HDMR18) based on the wBB proposal. The signature allows a signer to generate an anonymous signature $\sigma(sk_i, m)$ on a message m, where sk_i is the signer's private key. The protocol works as follows:

- $(pk, sk_m, spar) \leftarrow \texttt{Setup} \leftarrow (1^\kappa)$: On the input of the security parameter κ, the algorithm generates the system parameters $spar = (q, G_1, G_2, G_T, \mathbf{e}, g_1 \in G_1, g_2 \in G_2)$ satisfying $|q| = \kappa$. It also generates the manager's private key $sk_m \in_R Z_q$ and computes the public key $pk = g_2^{sk_m}$. It outputs the $(pk, spar)$ as a public output and the sk_m as the manager's private output.
- $(sk_i, RD) \leftarrow \texttt{KeyGen} \leftarrow (id_i, sk_m)$: On the input of manager's private key sk_m and signer's private identifier id_i, the protocol outputs the wBB signature $sk_i = g_1^{\frac{1}{sk_m + id_i}}$ to the signer and updates the manager's revocation database RD by storing id_i.
- $\sigma(sk_i, m) \leftarrow \texttt{Sign} \leftarrow (m, id_i, sk_i)$: On the input the signer's private identifier id_i, signer's private key sk_i, and the message m, the algorithm outputs the signature $\sigma(sk_i, m) = (g_1', sk_i', \bar{sk_i}, \pi)$, where:

- $g_1' = g_1^r$: The generator raised to a randomly chosen randomizer $r \in_R Z_q$.
- $sk_i' = sk_i^r$: The signers' private key raised to the randomizer.
- $\bar{sk_i} = {sk_i'}^{-id_i}$: The randomized private key raised to the signer identifier.
- $\pi = SK\{(id_i, r) : \bar{sk_i} = {sk_i'}^{-id_i} \wedge g_1' = g_1^r\}(m)$: The proof of knowledge of r and id_i signing the message m.

- $(0/1) \leftarrow \texttt{Verify} \leftarrow (\sigma(sk_i, m), m, pk, BL)$: On the input of the message m, its signature $\sigma(sk_i, m)$, a BlackList (BL), and the public key pk, the algorithm checks the proof of knowledge signature π and checks that the signature is valid with respect to the manager's public key using the equation $\mathbf{e}(\bar{sk_i} \cdot g_1', g_2) \stackrel{?}{=} \mathbf{e}(sk_i', pk)$. The collector also performs the revocation check $sk_i' \stackrel{?}{=} \bar{sk_i}^{id_i}$ for all id_i values stored on the BL. If the revocation check equation holds for any value on the blacklist, the signature is rejected. Otherwise, the signature is accepted if all other checks pass.

4.4 Partially Blind WI-Schnorr Signature

A form of digital signature known as a "blind signature" conceals the message's content from the signer. The resulting blind signature can then be publicly verified against the original (unblinded) message and used as a regular digital signature. This technology is mostly utilized in privacy-enhancing protocols where the message's owner and signer are separate entities. In a partially blind signature, the signer may include common public information in the signature (for example, an expiration date). So, the verifier needs the message, the common information, and the signature in order to verify the signature's authenticity. The WI-Schnorr signature, which is a partially blind signature based on the Schnorr protocol and maintains the Witnesses Indistinguishability (WI), was proposed by [1]. The WI-Schnorr signature is depicted in Figure 6. It is deemed that both the signer and the user have already agreed upon the public value "info".

4.5 Searchable Encryption: Outsourced Private Information Retrieval

A privacy enhancing technology that can facilitate privacy-preserving data processing is Searchable Encryption (SE), which enables storing a dataset in an encrypted form, while remaining searchable. This process relieves the service provider of the responsibility to maintain and protect the data from data breaches, as well as unauthorized use within the system.

Structured Encryption (STE) is a searchable encryption variation that provides balance between efficiency, functionality and security [35], [41]. Non-interactive STE schemes produce encrypted structures that can be queried using a single message containing a token, whereas in interactive schemes, queries

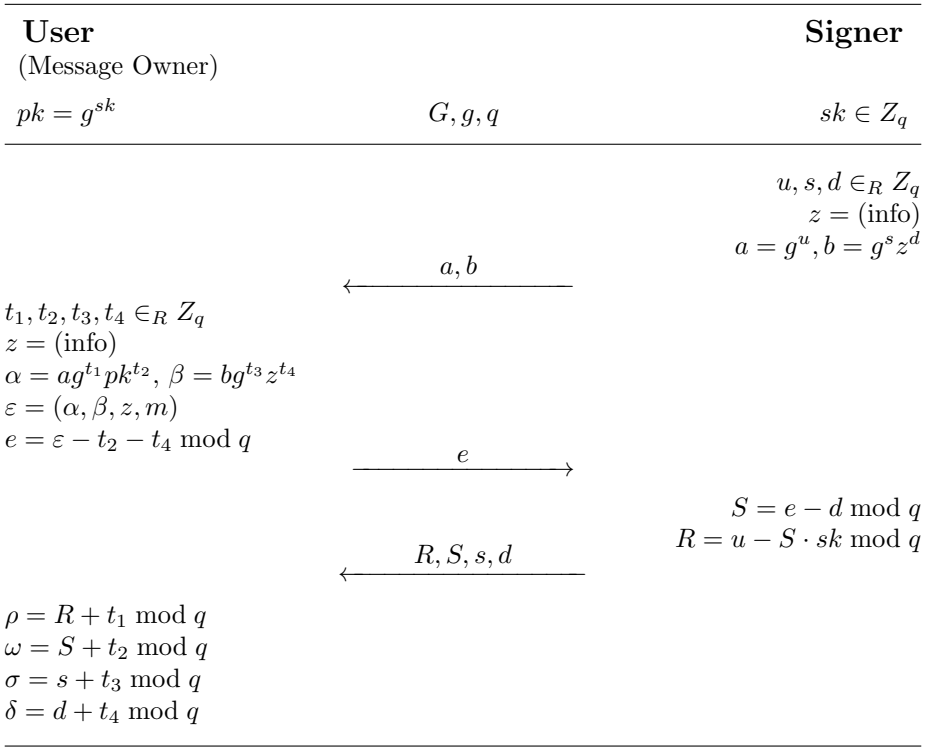

Figure 6: WI-Schnorr partially blind signature.

are performed through an interactive two-party protocol. Searchable Symmetric Encryption (SSE) schemes are a special case of STE that specializes for keyword search. In this setting, a data owner creates a data structure with efficient search support, such as an inverted index. Each document in the dataset is then encrypted, forming the Encrypted DataBase (EDB) and outsourced to an external search service. This enables performing queries on the dataset without revealing information about the dataset or the queries to the search service. The encrypted dataset consists of a list of document identifier and keyword-set pairs. Queries are performed using a search token, generated by the data owner, that allows the server to search through the index. A search query returns the document identifiers that satisfy the query expression. In general, an SSE scheme includes the following main algorithms [35], [42]:

- $(sk, \Delta) \leftarrow \texttt{Setup} \leftarrow (1^\kappa, DB)$: Using a security parameter κ as input and a database DB, consisting of a list of document identifiers and keywords, it outputs the secret key sk and an encrypted data structure Δ that will be outsourced to the data server. This algorithm varies depending on the specific SSE scheme and the data structures they use.

- $(\Gamma) \leftarrow$ `Token generation` $\leftarrow (sk, q)$: Using the secret key sk and the query q, it returns a query token Γ, to be used during search.
- $(\Phi) \leftarrow$ `Search` $\leftarrow (sk, q, \Gamma, \Delta)$: Using the secret key sk, the query q, and a search token Γ submitted by the user, the data server performs the search operations on encrypted data structure Δ, returning the matching documents. The algorithm outputs a set of encrypted documents Φ.

Depending on the SSE scheme, query expressiveness varies, supporting single-keyword, conjunctive, disjunctive or boolean queries.

5 Privacy-Preserving Parking Solution

In this section, we show how to integrate security and privacy features to the vehicle parking scenario introduced in Section 2. Furthermore, we answer the second research question, i.e., **RQ2:** How to build a privacy-preserving system which meets the requirements from RQ1? Which Privacy-Enhancing Technology (PET) can be used in order to protect users' privacy during using the system, i.e., reservation of parking slots and parking vehicle actions?

5.1 Detailed Description of Our Algorithms

In this section, we instantiate the algorithms and protocols of the privacy-preserving parking system presented in the previous section using the wBB signature [9] the Schnorr-like zero-knowledge protocol for proving the knowledge of a discrete logarithm [13] during the Parking vehicle phase. For the conversion from the proof of knowledge to the signature, we use the Fiat-Shamir heuristics [34]. We present the concrete algorithm and protocol instantiations below. To make our protocols easier to follow, we provide several illustrative figures (namely Figures 7, 8, 9, and 10) describing our protocols algorithmically and which can be read from top to bottom.

5.1.1 `Setup`

$(pk_{PSP}, sk_{PSP}, pk_{PLT}, sk_{PLT}, spar) \leftarrow$ `Setup` $\leftarrow (1^{\kappa})$: The purpose of this algorithm is to generate and set system parameters and cryptographic keys of the system. On the input of security parameter κ , the algorithm generates the public system parameters $spar$ (implicit input of all other algorithms), the public keys of the PSP and the PLTs shared by all users pk_{PSP}, pk_{PLT} and their private keys sk_{PSP}, sk_{PLT} which remain secret. The algorithm is run within the **Setup phase**, is initiated by the PSP, and runs between the PSP and all enrolled PSPs. The algorithms consists from two sub-algorithms, one run by PSP (called `SetupPSP`) and one run by PLT (called `SetupPLT`):

- $(pk_{PSP}, sk_{PSP}, spar) \leftarrow$ `SetupPSP` $\leftarrow (1^{\kappa})$: The algorithm inputs the security parameter κ and generates the bilinear group with parameters $spar = (q, G_1, G_2, G_T, \mathbf{e}, g_1, g_2)$ satisfying $|q| = \kappa$. It also generates the

PSP's private key $sk_{PSP} \in_R Z_q$ and computes the public key $pk_{PSP} = g_2^{sk_{PSP}}$. It outputs the $(pk_{PSP}, spar)$ as a public output and the sk_{PSP} as the PSP's private output. The algorithms is run by the PSP.

- $(pk_{PLT}, sk_{PLT}) \leftarrow$ `SetupPLT` $\leftarrow (spar)$: The algorithm inputs the system parameters $spar$ and generates the PLT's private key $sk_{PLT} \in_R Z_q$ and computes the public key $pk_{PLT} = g_1^{sk_{PLT}}$. It outputs the pk_{PLT} as a public output and the sk_{PLT} as the PLT's private output.

5.1.2 `Register`

$(\Lambda, sk_U, RD) \leftarrow$ `Register` $\leftarrow (ID, sk_{PSP}, spar)$: The purpose of this protocol is to add a new user to the system. The `Register` algorithm is presented in full notation in Figure 7. On the input of the PSP's private key sk_{PSP} and the user's identifier ID, the algorithm outputs the user's private key sk_U, user's access credential Λ and updates the PSP's revocation database RD. The algorithm is run within the **Registration phase** as an interactive protocol between the PSP and the user device. The system user is then able to require parking permits and access parking lots. The PSP inputs its private key sk_{PSP} and the user inputs the identity ID. If the ID is valid, the protocol generates user's private key $sk_U \in_R Z_q$ and outputs the wBB signature $\Lambda = g_1^{\frac{1}{sk_U + sk_{PSP}}}$ and the secret key sk_U to the user over a secure channel and updates the PSP's revocation database RD by storing $ID||sk_U$.

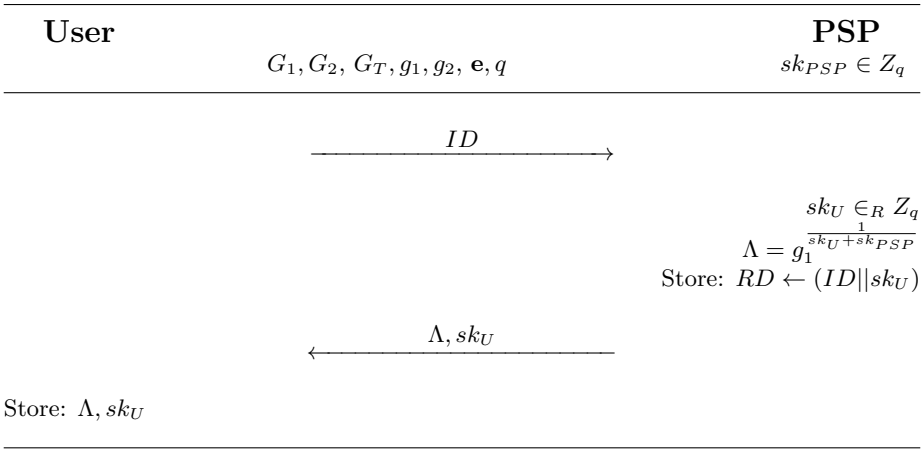

Figure 7: `Register` algorithm.

5.1.3 `Issue`

$(sk_{Cred}, CRED) \leftarrow$ `Issue` $\leftarrow (\Lambda, sk_{PLT}, pk_{PLT}, PD, spar)$: The parking permit is issued after the payment is done. The algorithm is run within the **Issue**

parking permit phase between the user device and the PLT through the PSP. The `Issue` algorithm is presented in full notation in Figure 8. The algorithm inputs the user's access credential Λ, user's parking data PD, the PLT's secret key sk_{PLT}, the PLT's public key pk_{PLT} and system parameters $spar$. It outputs the parking permit secret key sk_{Cred} and the parking permit $CRED$ that consists of the following elements $(\rho||\omega||\sigma||\delta||\hat{\Lambda}||\hat{g}||PD)$:

- $\hat{\Lambda}$: The user's access credential raised to a randomly chosen parking permit secret key $sk_{Cred} \in_R Z_q$, i.e. $\hat{\Lambda} = \Lambda^{sk_{Cred}}$.
- $\hat{g_1}$: The generator raised to a randomly chosen parking permit secret key $sk_{Cred} \in_R Z_q$, i.e. $\hat{g_1} = g_1^{sk_{Cred}}$.
- PD: The public parking data PD. The PD includes the PLT's identifier `PLTid`, parking time period `time_duration` and information about extended parking time `EPT`. To sign data, the PLT uses its secret key sk_{PLT}.
- $(\rho||\omega||\sigma||\delta)$: The PLT's signature on the user's partially blinded message, i.e., blinded values $\hat{\Lambda}$ and $\hat{g}$, and the public parking data PD. First, the PLT commits to the public data PD by computing commitments $a = g_1^u, b = g_1^s z^d$, where $z = \mathcal{F}(PD)$. Then, the user partially blinds the message. In particular, the user blinds the values $\hat{\Lambda}$ and $\hat{g}$ and computes commitments $\alpha = a g_1^{t_1} pk_{PLT}^{t_2}$, $\beta = b g_1^{t_3} z^{t_4}$ using the PLT's public key pk_{PLT}, the PLT's commitments (a, b) and the public data $z = \mathcal{F}(PD)$. The user generates the hash ϵ on all these data, derives value e from ϵ, and sends it to the PLT. The PLT computes blind signature (R, S, s, d) on value e using its secret key sk_{PLT}. Finally, the user unblind the blind signature and obtains the signature $(\rho||\omega||\sigma||\delta)$.

The parking permit includes blinded user's access token $\hat{\Lambda}$, and therefore, it cannot be used for user identification by PSP in this phase.

5.1.4 `Verify`

$(0/1) \leftarrow$ `Verify` $\leftarrow (sk_U, sk_{Cred}, \Lambda, CRED, pk_{PLT}, pk_{PSP}, spar)$: The parking is anonymous and unlinkable since the parking permit does not include any linkable or personal information. The algorithm is run within the **Parking vehicle phase** between the user device and the PLT. The `Verify` algorithm is presented in CS notation in Figure 9. The algorithm inputs the user's secret key sk_U, the parking permit secret key sk_{Cred}, the user's access credential Λ, the parking permit $CRED$, the PSP's public key pk_{PSP}, the PLT's public key pk_{PLT}, and system parameters $spar$. It checks that the signature on parking permit is valid under the PLT's public key using the equation $\varepsilon = \omega + \delta \stackrel{?}{=} \mathcal{H}(g_1^\rho pk_{PLT}^\omega || g_1^\sigma \mathcal{F}(PD)^\delta || \mathcal{F}(PD) || \bar{\Lambda} || \hat{\Lambda} || \hat{g})$. If the signature is valid, the algorithm checks the proof of knowledge π and validity of the user's access credential Λ with respect to the PSP's public key using the equation $\mathbf{e}(\bar{\Lambda} \cdot \hat{g_1}, g_2) \stackrel{?}{=} \mathbf{e}(\hat{\Lambda}, pk_{PSP})$. If all checks pass, the parking permit is accepted.

User	**PSP**	**PLT**
$\Lambda, sk_U, pk_{PLT} = g_1^{sk_{PLT}}$	$G_1, G_2, G_T, g_1, g_2, \mathbf{e}, q$	$sk_{PLT} \in Z_q$

$sk_{Cred} \in_R Z_q$
$\hat{\Lambda} = \Lambda^{sk_{Cred}}$
$\bar{\Lambda} = \hat{\Lambda}^{-sk_U}$
$\hat{g_1} = g_1^{sk_{Cred}}$

$u, s, d \in_R Z_q$
$PD = \{\texttt{PPID}||\texttt{PLTid}||\texttt{time\_duration}||\texttt{EPT}\}$
$z = \mathcal{F}(PD))$
$a = g_1^u, b = g_1^s z^d$

$\xleftarrow{a, b}$

$t_1, t_2, t_3, t_4 \in_R Z_q$
$PD = \{\texttt{PPID}||\texttt{PLTid}||\texttt{time\_duration}||\texttt{EPT}\}$
$z = \mathcal{F}(PD)$
$\alpha = a g_1^{t_1} pk_{PLT}^{t_2}$, $\beta = b g_1^{t_3} z^{t_4}$
$\varepsilon = \mathcal{H}(\alpha||\beta||z||\bar{\Lambda}||\hat{\Lambda}||\hat{g})$
$e = \varepsilon - t_2 - t_4 \bmod q$

$\xrightarrow{e}$

$S = e - d \bmod q$
$R = u - S \cdot sk_{PLT} \bmod q$

$\xleftarrow{R, S, s, d}$

$\rho = R + t_1 \bmod q$
$\omega = S + t_2 \bmod q$
$\sigma = s + t_3 \bmod q$
$\delta = d + t_4 \bmod q$

Store: $sk_{Cred}, CRED = (\rho||\omega||\sigma||\delta||\bar{\Lambda}||\hat{\Lambda}||\hat{g}||PD)$

Figure 8: `Issue` algorithm.

Otherwise, the parking permit is rejected. The proof of knowledge protocol is run as follow:

- The PLT generates random authentication challenge $c \in_R Z_q$ and send it to the user.

- The user compute proof of knowledge π and sends it to PLT:

$$\begin{aligned}
\rho_{SkCred}, \rho_{SkU} &\in_R Z_q \\
t &= \hat{\Lambda}^{\rho_{SkU}} g_1^{\rho_{SkCred}} \\
e &= \mathcal{H}(\hat{g_1}, \hat{\Lambda}, \bar{\Lambda}, t, c) \\
s_{SkCred} &= \rho_{SkCred} - e \cdot sk_{Cred} \\
s_{SkU} &= \rho_{SkU} + e \cdot sk_U \\
\pi &= (e, s_{SkCred}, s_{SkU})
\end{aligned}$$

- The PLT verifies the proof of knowledge π:

$$\begin{aligned}
\widehat{t} &= (\bar{\Lambda} \cdot \hat{g_1})^e \hat{\Lambda}^{s_{SkU}} \cdot g_1^{s_{SkCred}} \\
e &\stackrel{?}{=} \mathcal{H}(\hat{g_1}, \hat{\Lambda}, \bar{\Lambda}, \widehat{t}, c)
\end{aligned}$$

User	**PLT**
$sk_U, sk_{Cred}, \Lambda, CRED$	$pk_{PLT} = g_1^{sk_{PLT}}, pk_{PSP} = g_2^{sk_{PSP}}$
$G_1, G_2, G_T, g_1, g_2, \mathbf{e}, q$	
$\xrightarrow{\qquad CRED \qquad}$	
	$PD = \{\texttt{PPID}\|\|\texttt{PLTid}\|\|\texttt{time\_duration}\|\|\texttt{EPT}\}$
	$\varepsilon = \omega + \delta \stackrel{?}{=} \mathcal{H}(g_1^{\rho} pk_{PLT}^{\omega} \|\| g_1^{\sigma} \mathcal{F}(PD)^{\delta} \|\| \mathcal{F}(PD) \|\| \bar{\Lambda} \|\| \hat{\Lambda} \|\| \hat{g})$
$\xleftarrow{\qquad \pi = SK\{(sk_U, sk_{Cred}) : \bar{\Lambda} = \hat{\Lambda}^{-sk_U} \wedge \hat{g_1} = g_1^{sk_{Cred}}\}(c) \qquad}$	
	Check π
	$\mathbf{e}(\bar{\Lambda} \cdot \hat{g_1}, g_2) \stackrel{?}{=} \mathbf{e}(\hat{\Lambda}, pk_{PSP})$

Figure 9: `Verify` algorithm.

5.1.5 `Update`

$(sk_{Cred}, CRED) \leftarrow$ `Update` $\leftarrow (sk_U, sk_{Cred}, \Lambda, CRED, pk_{PLT}, pk_{PSP}, sk_{PLT}, \texttt{EPT}, spar)$: The purpose of this protocol is to extend parking time of a parking permit. The algorithm inputs the user's secret key sk_U, the parking permit secret key sk_{Cred}, the user's access credential Λ, the parking permit $CRED$, the PSP's public key pk_{PSP}, the PLT's public key pk_{PLT}, the PLT's secret key sk_{PLT}, the extension parking time `EPT`, and system parameters $spar$. The algorithm is run in two steps.

1. $(0/1) \leftarrow$ `Verify` $\leftarrow (sk_U, sk_{Cred}, \Lambda, CRED, pk_{PLT}, pk_{PSP}, spar)$: The `Verify` algorithm is run first. The user specifies the parking permit $CRED$ for extension parking time by sending `PLTid` and `PPID` information. The PLT finds corresponding parking permit $CRED$ in its database and stars the `Verify` algorithm. If verification is successful, then the algorithm continues, ends otherwise.

2. $(sk_{Cred}, CRED) \leftarrow$ `Issue` $\leftarrow (\Lambda, sk_{PLT}, pk_{PLT}, PD, spar)$: The `Issue` algorithm is run second. The user chooses and sends a new expiration parking time `ETP` to PLT. Then, the user and the PLT run together `Issue` algorithm using the PD from the old user's parking permit $CRED$ and new `ETP` to create a new extended parking permit $CRED$.

5.1.6 `Revoke`

$(ID) \leftarrow$ `Revoke` $\leftarrow (CRED, RD, spar)$: Thanks to this algorithm, the PSP can identify malicious users from the parking permits using the revocation database RD. The algorithm is run within the **Revocation phase** by the PSP. The algorithm inputs parking permit $CRED$ and PSP's revocation database RD. It checks $\bar{\Lambda} \stackrel{?}{=} \hat{\Lambda}^{-sk_U}$ for all sk_U in RD. The sk_U that holds in the equation is linked with the user's identifier ID. By providing the ID to an identity provider, the PSP can revoke malicious users' anonymity and identify the users.

5.2 Optional Extension of the system supporting the non-repudiation feature

The proposal of the parking system presented in Section 5.1 does not provide non-repudiation features. In fact, the PSP knows all secret keys sk_U of all system users. Thanks to this knowledge, the PSP can revoke users by running the `Revoke` algorithm. On the other hand, the malicious PSP can forge valid parking permits for all system users, and therefore, falsely accused of committing a crime on anyone in the system. Due to this fact, the PSP must be trusted and honest. However, if the system implementer requires non-repudiation features, we have proposed a solution as well. The solution is based on using a secure two-party computation of wBB signature within the `Register` algorithm. We refer to [6] and [56] for more details. Our extension impacts only `Registration` and `Revoke` algorithms presented in Section 5.1. The other algorithms remain unchanged. The extended `Registration` algorithm is depicted in Figure 10.

The algorithm takes on the input system parameters $spar = (q, G_1, G_2, G_T, \mathbf{e}, g_1, g_2)$ and parameters $(\mathbf{g}, \mathbf{h}, \mathbf{n}, \mathfrak{g}, \mathfrak{h}, \mathfrak{n})$ [6], where $\mathbf{n}$ is RSA-modulus of size at least $2^{3\kappa}q^2$, κ is a security parameter, $\mathbf{h} = \mathbf{n} + 1$, $\mathbf{g}$ is an element of the order $\phi(\mathbf{n}) \bmod \mathbf{n}^2$, $\mathfrak{n}$ is RSA modulus such that neither the user nor the PSP knows its factors (e.g., $\mathfrak{n}$ can be provided by a TTP), $\mathfrak{h}$ and $\mathfrak{g}$ are two elements in $Z^*_{\mathfrak{n}}$ such that $\log_{\mathfrak{g}} \mathfrak{h}$ is unknown and $\mathfrak{g} \in \langle \mathfrak{h} \rangle$. The algorithm is run by the user and the PSP as in main scheme and allows computing user's access credential $\Lambda = g_1^{1/(sk_{PSP}+sk_U)}$ without that the PSP reveals its private key

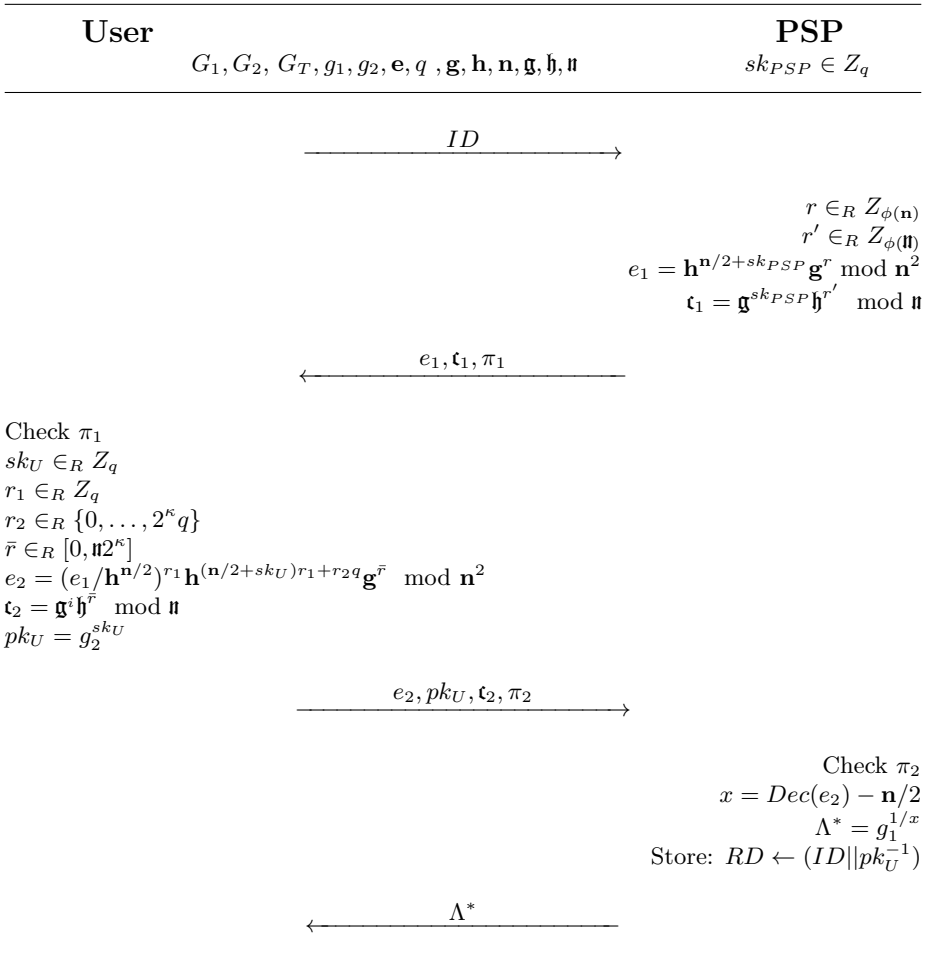

Figure 10: `Register` algorithm implementing non-repudiation feature to the parking system.

sk_{PSP} and the user its secret key sk_U. The algorithm is based on homomorphism of Paillier cryptosystem [52]. Fist, the PSP homomorphicly encrypts its secret key sk_{PSP} by computing $e_1 = \mathbf{h}^{\mathbf{n}/2+sk_{PSP}}\mathbf{g}^r \bmod \mathbf{n}^2$ and computes commitment $\mathfrak{c}_1 = \mathfrak{g}^{sk_m}\mathfrak{h}^{r'} \bmod \mathfrak{n}$. Then, the PSP and the user run the PK protocol:

$$\pi_1 = PK\{(sk_{PSP}, r, r') : e_1/\mathbf{h}^{\mathbf{n}/2} = \mathbf{h}^{sk_{PSP}}\mathbf{g}^r \bmod \mathbf{n}^2 \\ \wedge\ \mathfrak{c}_1 = \mathfrak{g}^{sk_{PSP}}\mathfrak{h}^{r'} \bmod \mathfrak{n}\}$$

If the proof π_1 is accepted by the user, the user homomorphicly encrypts its secret key sk_U by computing $e_2 = (e_1/\mathbf{h}^{\mathbf{n}/2})^{r_1}\mathbf{h}^{(\mathbf{n}/2+sk_U)r_1+r_2q}\mathbf{g}^{\bar{r}} \mod \mathbf{n}^2$ and computes commitment $\mathfrak{c}_2 = \mathfrak{g}^i\mathfrak{h}^{\bar{r}} \mod \mathfrak{n}$ and its public key $pk_U = g_2^{sk_U}$. Then, the PSP and the user run the PK protocol:

$$\begin{aligned}\pi_2 = PK\{(sk_U, r_1, r_2, sk'_U, u, \bar{r}) : e_2/\mathbf{h}^{\mathbf{n}/2} &= (e_1/\mathbf{h}^{\mathbf{n}/2})^{r_1}\mathbf{h}^{sk'_U}(\mathbf{h}^q)^{r_2}\mathbf{g}^{\bar{r}} \mod \mathbf{n}^2 \\ \wedge\ \mathfrak{c}_2 &= \mathfrak{g}^{sk_U}\mathfrak{h}^{\bar{r}} \mod \mathfrak{n} \\ \wedge\ 1 &= \mathfrak{c}_2^{r_1}(1/\mathfrak{g})^{sk'_U}\mathfrak{h}^u \mod \mathfrak{n} \\ \wedge\ pk_U &= g_2^{sk_U}\}.\end{aligned}$$

If the proof π_2 is accepted by the PSP, the PSP decrypts (i.e., Paillier decryption) $x = Dec(e_2) - \mathbf{n}/2$, computes $\Lambda^* = g_1^{1/x}$ and sends it to the user. The user computes $\Lambda = (\Lambda^*)^{r_1}$ and verifies that it is a correct signature on sk_U, i.e. $\Lambda = g_1^{\frac{1}{sk_U+sk_{PSP}}}$ holds.

The PSP can open the parking permit $CRED$ and track the malicious users by running the modified `Revoke` algorithm. With the PSP's revocation database RD and the parking permit $CRED$, the PSP checks if the equation $\mathbf{e}(\hat{\Lambda}, pk_U^{-1}) \stackrel{?}{=} \mathbf{e}(\bar{\Lambda}, g_2)$ holds for any of pk_U in its RD. If there exists an pk_U for which this equation holds, pk_U is linked with the user's ID, which is then sent to the corresponding identity provider to identify the user.

5.3 Security and Privacy Analysis

The proposed system is built on provable secure cryptographic primitives such as wBB signature [9], group signature [38], partially blind WI-Schnorr signature [1] and secure two-party computation of wBB signature [6]. We refer to these papers for more details on their security analyses. In the security and privacy analysis of our proposal, we adopt the attacker model for the privacy-preserving parking system defined in [21] and apply it to our security and privacy requirements defined in Section 2. The attacker model considers both internal and external adversaries. In the case of internal attackers, the PSP and the PLT are considered honest-but-curious, while users can act maliciously. Entities omitting the proposed protocols to commit fraud are considered external attackers. Considering this adversary model, we get the security and privacy properties of our system and how they are fulfilled. Note that, we define four lemmas that are in line with our requirements from Section 2. See Section 2 for more details. Namely, Lemma 5.1 is in line with **Conditional traceability** and **Revocation** requirements, Lemma 5.2 is in line with **Data confidentiality**, **Data privacy**, **Pseudonymity**, and **Unlinkability** requirements, Lemma 5.3 is in line with **Authentication** requirement, and Lemma 5.4 is in line with **Data authenticity integrity** requirements.

Lemma 5.1. ***Revocable anonymity****: Users' privacy is preserved as long as they do not try to commit fraud, in which case they can be identified.*

Proof. During the **Issue parking permit phase**, users provide their unique access credential Λ to the PLT through the PSP. This credential is blinded, and therefore, the PLT and the PSP can learn nothing about it. Furthermore, the access credential Λ is stored in the parking permit $CRED$, which is presented by the user to the PLT within the **Park vehicle phase**. However, in this case, the users' credentials are randomized, and therefore, mutually unlikable by the PLT. The revocation is possible thanks to $(\bar{\Lambda}||\hat{\Lambda})$ values stored in the parking permit $CRED$. With these two values, the PSP can perform the `Revoke` algorithm and identify the users. Users traceability by the PSP is possible:

1. **Main scheme (see Section 5.1)**: The PSP checks $\bar{\Lambda} \stackrel{?}{=} \hat{\Lambda}^{-sk_{U \in RD}}$ for all $sk_{U \in RD}$ in RD. If any $sk_{U \in RD}$ holds in the equation then $sk_{U \in RD} = sk_U$ and $sk_{U \in RD}$ is linked with the user's identifier ID:

$$\bar{\Lambda} = \hat{\Lambda}^{-sk_U} \stackrel{?}{=} \hat{\Lambda}^{-sk_{U \in RD}}$$

2. **Extended scheme (see Section 5.2)**: The PSP checks $\mathbf{e}(\hat{\Lambda}, pk_{U \in RD}^{-1}) \stackrel{?}{=} \mathbf{e}(\bar{\Lambda}, g_2)$ for all $pk_{U \in RD}^{-1}$ in RD. If any $pk_{U \in RD}^{-1}$ holds in the equation then the user used corresponding sk_U and $pk_{U \in RD}^{-1}$ is linked with the user's identifier ID:

$$\mathbf{e}(\hat{\Lambda}, pk_{U \in RD}^{-1}) = \mathbf{e}(\hat{\Lambda}, g_2^{-sk_U \in RD}) = \mathbf{e}(\hat{\Lambda}, g_2)^{-sk_U \in RD} \stackrel{?}{=} \mathbf{e}(\bar{\Lambda}, g_2) = \mathbf{e}(\hat{\Lambda}^{-sk_U}, g_2) = \mathbf{e}(\hat{\Lambda}, g_2)^{-sk_U}$$

□

Lemma 5.2. ***Non-traceable and unlinkable reservations****: User's actions cannot be bound together by third parties.*

Proof. The PLT is receiving anonymous blinded user's access credential within the **Issue parking permit phase** and anonymous randomized user's access credential within the **Parking vehicle phase**. No personal or other linkable information is provided during these processes. Due to this fact, the PLT cannot bind any subsequent parking reservation requests of the user. In the same vein, as user's revocable data $(\bar{\Lambda}||\hat{\Lambda})$ are stored in the parking permit $CRED$ and only provided to the PSP in case of a fraud attempt, neither the PSP can link user's reservations. The parking permit is always anonymous and unlinkable due to the zero-knowledge property of the proof of knowledge protocol. Distribution of $\hat{\Lambda}$, $\bar{\Lambda}$, $\hat{g_1}$ is random and uniform in Z_q as sk_{Cred} is selected randomly and uniformly from Z_q:

$$\hat{\Lambda} = \Lambda^{sk_{Cred}}$$
$$\bar{\Lambda} = \hat{\Lambda}^{-sk_U}$$
$$\hat{g_1} = g_1^{sk_{Cred}}$$

□

Lemma 5.3. ***Fraud avoidance****: A user cannot be falsely inquired about not completing a payment process.*

Proof. The **Issue parking permit phase** is run after the payment for parking is made. The parking permit $CRED$ includes the paid parking time, so, any false accusation from the PLT can be denied. □

Lemma 5.4. ***Non-repudiation and integrity****: Evidences generated from entities interaction can be neither denied nor counterfeited.*

Proof. The PLT proofs its identity by signing the parking permit $CRED$, the PSP proofs its identity by signing the user's access credential Λ, and the user proofs the possession of a valid secret keys sk_U and sk_{Cred} within the **Parking vehicle phase**. As a result of the **Issue parking permit phase**, only the user obtains complete parking permit $CRED$, containing the parking reservation details PD and revocable data $(\bar{\Lambda}||\hat{\Lambda})$. The PLT gets only partial information about $CRED$ (namely PD consists of `PPID`, `PLTid`, `time_duration`, `EPT`). The PLT signs PD with blind signature scheme. The signature validity can be verified by everyone, therefore, proofs' integrity is granted.

The signature on a parking permit $CRED$ is always accepted if a valid PLT's secret key is used in the signature:

$$\varepsilon = \mathcal{H}(\alpha||\beta||z||\bar{\Lambda}||\hat{\Lambda}||\hat{g}) \stackrel{?}{=} \omega + \delta \stackrel{?}{=} \mathcal{H}(g_1^{\rho} pk_{PLT}^{\omega}||g_1^{\sigma}\mathcal{F}(PD)^{\delta}||\mathcal{F}(PD)||\bar{\Lambda}||\hat{\Lambda}||\hat{g})$$

$$\begin{aligned}
\alpha = a g_1^{t_1} pk_{PLT}^{t_2} &\stackrel{?}{=} g_1^{\rho} pk_{PLT}^{\omega} \\
&= g_1^{(R+t_1)} pk_{PLT}^{(S+t_2)} \\
&= g_1^{(u-(e-d)\cdot sk_{PLT}+t_1)} pk_{PLT}^{(e-d+t_2)} \\
&= g_1^{u} pk_{PLT}^{(-e+d)} g_1^{t_1} pk_{PLT}^{(e-d+t_2)} \\
&= a g_1^{t_1} pk_{PLT}^{t_2} \\
\beta = b g_1^{t_3} z^{t_4} &\stackrel{?}{=} g_1^{\sigma}\mathcal{F}(PD)^{\delta} \\
&= g_1^{(s+t_3)} z^{(d+t_4)} \\
&= g_1^{s} z^{d} g_1^{t_3} z^{t_4} \\
&= b g_1^{t_3} z^{t_4} \\
\varepsilon = e + t_2 + t_4 &\stackrel{?}{=} \omega + \delta \\
&= S + t_2 + d + t_4 \\
&= e - d + t_2 + d + t_4 = e + t_2 + t_4
\end{aligned}$$

The signature on randomized user's access credential Λ is always accepted

if a valid PSP's secret key is used in the signature:

$$\begin{aligned}
\mathbf{e}(\bar{\Lambda} \cdot \hat{g_1}, g_2) &\stackrel{?}{=} \mathbf{e}(\hat{\Lambda}, pk_{PSP}) \\
\mathbf{e}(\Lambda^{-sk_U \cdot sk_{Cred}} g_1^{sk_{Cred}}, g_2) &= \mathbf{e}(\Lambda^{sk_{Cred}}, g_2^{sk_{PSP}}) \\
\mathbf{e}(g_1^{\frac{-sk_U \cdot sk_{Cred}}{sk_{PSP}+sk_U}} g_1^{sk_{Cred}}, g_2) &= \mathbf{e}(\Lambda^{sk_{Cred}}, g_2^{sk_{PSP}}) \\
\mathbf{e}(g_1^{\frac{sk_{PSP} \cdot sk_{Cred} + sk_U \cdot sk_{Cred} - sk_U \cdot sk_{Cred}}{sk_{PSP}+sk_U}}, g_2) &= \mathbf{e}(\Lambda^{sk_{Cred}}, g_2^{sk_{PSP}}) \\
\mathbf{e}(\Lambda^{sk_{PSP} \cdot sk_{Cred}}, g_2) &= \mathbf{e}(\Lambda^{sk_{Cred}}, g_2^{sk_{PSP}}) \\
\mathbf{e}(\Lambda, g_2)^{sk_{PSP} \cdot sk_{Cred}} &= \mathbf{e}(\Lambda, g_2)^{sk_{PSP} \cdot sk_{Cred}}
\end{aligned}$$

The proof $\pi = SK\{(sk_U, sk_{Cred}) : \bar{\Lambda} = \hat{\Lambda}^{-sk_U} \wedge \hat{g_1} = g_1^{sk_{Cred}}\}(c)$ is always accepted if valid user's secret keys sk_U, sk_{Cred} are used in the proof:

$$\begin{aligned}
e = \mathcal{H}(\hat{g_1}, \hat{\Lambda}, \bar{\Lambda}, t, c) &\stackrel{?}{=} \mathcal{H}(\hat{g_1}, \hat{\Lambda}, \bar{\Lambda}, \widehat{t}, c) \\
t = \hat{\Lambda}^{\rho_{SkU}} g_1^{\rho_{SkCred}} &\stackrel{?}{=} (\bar{\Lambda} \cdot \hat{g_1})^e \hat{\Lambda}^{s_{SkU}} \cdot g_1^{s_{SkCred}} = \widehat{t} \\
&= (\hat{\Lambda}^{-e \cdot sk_U} \cdot g_1^{e \cdot sk_{Cred}}) \hat{\Lambda}^{(\rho_{SkU} + e \cdot sk_U)} \cdot g_1^{(\rho_{SkCred} - e \cdot sk_{Cred})} \\
&= \hat{\Lambda}^{\rho_{SkU}} \cdot g_1^{\rho_{SkCred}}
\end{aligned}$$

□

5.4 Experimental results

In this section, we provide our experimental results. In particular, we show the efficiency of our proposal on Android devices. We use the Android phones: Honor 8X (chip: Kirin 810, OS: Android 10, RAM: 4 GB) and OnePlus Nord 5G (chip: Snapdragon 765G, OS: Android 11, RAM: 8 GB). In order to perform cryptographic operations, we use the MCL [58] ++ library (using C++17 version of the ISO/IEC 14882 standard) and Android Native Development Kit (NDK). The Android NDK allows us to execute a program in C/C++ on Android devices instead of using Java libraries, and therefore, to achieve better performance results. The source code of the Android application is available online on the GitLab repository[7]. Our benchmark test on both phones for different arithmetic operations and fields is presented in Table 2. We measure the time complexity of each MCL operation 10 times and then compute the median from these data. From the table, we can see that the time complexity of operations in F_r is negligible. They take approximately 30 μs for the BN254 elliptic curve on OnePlus Nord 5G. A similar situation is in the case of operations in G_1 and G_2. The most expensive operations are scalar multiplication `mul1`, `mul2`, modular exponentiation `powT`, and bilinear pairings `pairT`. These operations have a significant impact on the time complexity of the whole protocol.

[7] `https://gitlab.com/brno-axe/tacr-crypto/android-mcl-test`

Table 2: Benchmark tests of MCL library operations (modular arithmetic and elliptic curve) on Android devices.

Device:		OnePlus Nord 5G		Honor 8X	
Elliptic curve:		BN254 [ms]	BLS12_381 [ms]	BN254 [ms]	BLS12_381 [ms]
F_r	`addF` (addition)	0.051	0.040	0.036	0.130
	`subF` (subtraction)	0.029	0.023	0.035	0.032
	`mulF` (multiplication)	0.025	0.019	0.027	0.023
	`divF` (division)	0.081	0.091	0.145	0.149
	`negF` (negation)	0.016	0.019	0.020	0.023
G_1	`add1` (addition)	0.021	0.046	0.054	0.120
	`sub1` (subtraction)	0.022	0.034	0.037	0.058
	`mul1` (multiplication)	0.537	1.056	0.576	0.115
	`dbl1` (doubling)	0.020	0.024	0.066	0.023
	`neg1` (negation)	0.016	0.018	0.020	0.020
G_2	`add2` (addition)	0.030	0.064	0.058	0.166
	`sub2` (subtraction)	0.027	0.052	0.039	0.106
	`mul2` (multiplication)	0.397	2.135	1.196	2.597
	`dbl2` (doubling)	0.022	0.034	0.100	0.115
	`neg2` (negation)	0.014	0.017	0.023	0.029
G_T	`powT` (power)	1.545	2.843	2.070	3.667
	`mulT` (multiplication)	0.040	0.061	0.102	0.142
	`pairT` (pairing)	2.808	7.527	3.025	9.687

Note: F_r represents finite field Z_q, G_1 is cyclic additive group of order q generated by elliptic curve, G_2 is cyclic additive group of order q generated by elliptic curve, G_T is the cyclic multiplicative group of order q.

To show the complexity of our system, we sum up the algebraic operations used in the cryptographic algorithm (i.e., `Register`, `Issue`, `Verify`, `Update` and `Revoke`) for each involved system entity and compute the execution time. To do so, we used data from Table 2. In particular, we consider using the OnePlus Nord 5G Android device and the BN254 elliptic curve. Considering our results in the Table 3, the cryptographic core time complexity is negligible, since it takes ca. 6 ms for `Issue`, ca. 9 ms for `Verify` and ca. 14 ms for `Update` algorithm.

The complexity of the `Revoke` algorithm is linearly dependent on the number of users in the system. The time complexity of `Revoke` algorithm for both main scheme (see Section 5.1) and extended scheme (see Section 5.2) based on number of system user is depicted in Figure 11. The main algorithm requires performance of N operations of `mul1`, while the extended algorithm requires the performance of N operations of `pairT`), where N is a number of system users. If we consider OnePlus Nord 5G Android device and 1 million system users, the `Revoke` algorithm will need ca. 9 min (i.e., main algorithm) and

Table 3: Computation complexity of the cryptographic algorithms.

Algorithm	User		PSP		Total
	Operations	Time [ms]	Operations	Time [ms]	Time [ms]
`Register`	-	-	1x`mul1`, 1x`addF` 1x`divF`	0.669	0.669
Algorithm	User		PLT		Total
	Operations	Time [ms]	Operations	Time [ms]	Time [ms]
`Issue`	7x`mul1`, 4x`add1` 2x`subF`, 4x`addF`	4.107	3x`mul1`, 1x`add1` 2x`subF`, 1x`mulF`	1.715	5.821
`Verify`	2x`mul1`, 1x`add1`, 1x`addF`, 2x`mulF` 1x`subF`	1.225	3x`mul1`, 3x`add1` 2x`pairT`	7.290	8.515
`Update`	9x`mul1`, 5x`add1`, 5x`addF`, 2x`mulF` 3x`subF`	5.331	6x`mul1`, 4x`add1` 2x`subF`, 1x`mulF`, 2x`pairT`	9.005	14.336

ca. 47 min (i.e., extended algorithm) to identify a malicious user. By using more powerful servers and palatalization techniques, the revocation time can be reduced significantly.

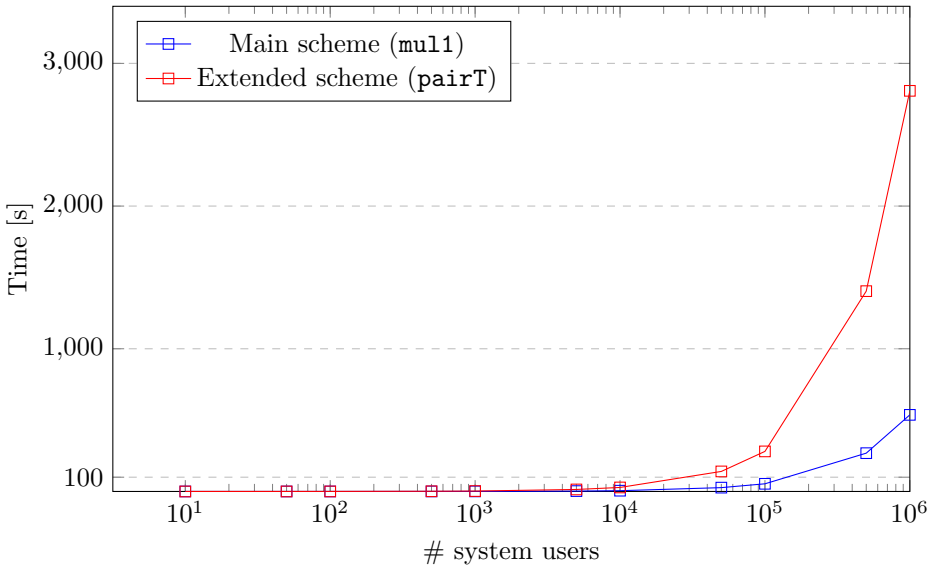

Figure 11: Time complexity of `Revoke` algorithm.

6 Privacy Preserving Data Processing for Statistics Analysis

During the use of the parking system, transaction data is produced, the processing of which could provide interesting information about the characteristics of the service and possible improvements. This processing, however, needs to be performed in a privacy-preserving way, in order to reap the benefits of this processing without compromising the privacy of the users. To solve this requirement, we need to answer the third research question, i.e., **RQ3:** How to allow third parties to perform statistical analyses on the parking transaction data, in a privacy preserving way? Which PET can be used to support this task? In the context of the parking scenario, data remain in a clear-text form during the course of a transaction, but once the transaction is completed, the transaction record is moved to long term storage in encrypted form for privacy-preserving statistical analysis. Additionally, following the data minimisation principle, only the necessary data items for analysing the service use is stored in the transaction records. In particular, a parking transaction record includes the following data items:

- **Vehicle classification**: It defines official classification categories used in vehicle licenses.
- **Vehicle type**: It can represent the vehicle power supply, e.g. gas, electric, GPL.
- **Parking spot type**: It can represent the disability spot, premium spot, short duration spot, long duration spot, secure/closed spot.
- **Services required**: It can indicate washing, charging or any other needs.
- **User affiliation**: It can indicate affiliation with companies/venues, used for special pricing.
- **Parking start timestamp**: Time when parking started and the user has access to the parking lot.
- **Parking end timestamp**: Time when parking has ended and the user must leave the parking lot.
- **Parking transaction cost**: The price that the user must pay for the parking time in the selected parking lot.

Using these data items as search keywords, statistics can be extracted on parking spot demand, peak hours and availability. These statistics can facilitate decisions on pricing strategies and parking spots allocation and management, as well as possible custom offers and packages for specific companies/venues.

The objective of our scheme is to support the following functional and efficiency requirements, additionally to the security and privacy requirements identified in Section 2.4, as they are desired for the SSE scheme and appropriate for the parking scenario:

- **Multi-user functionality**: Searching the dataset is possible for authorized third parties other than the data owner.
- **Query expressiveness (boolean query support)**: Complex queries need to be supported to enable extracting useful statistics from the dataset.
- **Efficiency**: The search functionality needs to be efficient and scalable, in order for the solution to be applicable in practice.

We propose our MC-SSE scheme (for Multi-Client SSE scheme), which extends the efficient and expressive BIEX SSE scheme [42] with the multi-user functionality, not supported by the original BIEX scheme. An open source library of the BIEX SSE scheme, known as Clusion[8], is publicly available, which is particularly attractive in the idea of proposing an extension with experimental results.

6.1 Our MC-SSE System Model and Overview

The following entities are interacting in the data processing system for the parking scenario, as illustrated in Figure 12:

- **The data owner (D)**: The data owner creates an encrypted dataset and outsources it. In our scenario the PLT acts as the data owner.
- **The storage and query server (S)**: They handle the encrypted dataset storage and performs queries on it.
- **Search clients (C)**: They are allowed to search on the encrypted dataset. The PSP, other PLTs in the parking system, or any other interested stakeholder can act as a search client.

To achieve the multi-client extension of BIEX, the data owner provides Search clients an authorization token that enables them to create search tokens and submit queries to the Server limited by the keywords contained in the authorization token. With this extension the properties of the BIEX scheme are preserved, i.e. boolean query support with efficient search, while enabling multi-client functionality.

6.2 Refining the Security and Privacy Threat Model

As considered in classical SSE schemes, the Server S is honest-but-curious, thus fulfilling the search tasks over the database correctly, but attempting to collect as much data as possible. The Clients C are malicious and the data owner D is honest. We only consider internal attackers as all the channels between any interacting entities - D-S, D-C and S-C - are authenticated.

In the light of the system model of Section 6.1, additionally to the security and privacy requirements identified in Section 2.4 - data minimisation, index and

[8]Clusion library: https://github.com/encryptedsystems/Clusion

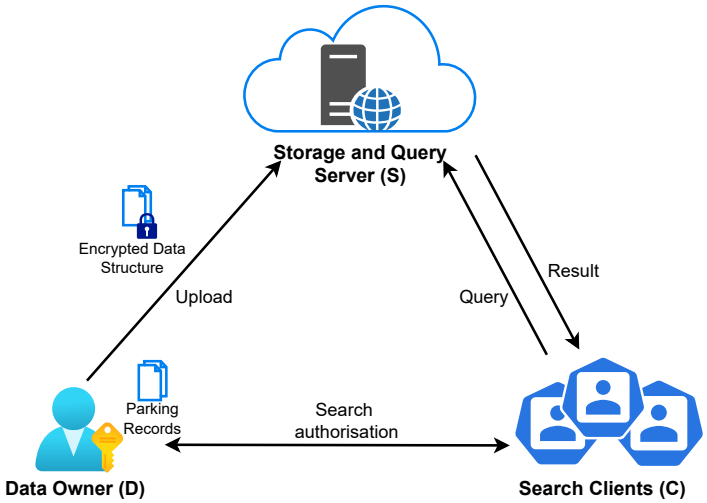

Figure 12: Multi-client SSE functionality.

document privacy, query privacy, access pattern privacy, the query authorization requirement is revisited for the multi-client SSE scheme as follows:

- **Query authorization**: Only authorized clients on authorized keywords are able to extract statistics from the server.
- **Privilege escalation prevention, as a sublease of the query authorization issue**: Clients must not be able to collude for generating a search token with a superset of combined keywords.

6.3 Our MC-SSE Algorithms

The Multi-Client SSE (MC-SSE) scheme consists of the following algorithms:

- $(sk, \mathsf{EDX}, \mathsf{EMM}) \leftarrow \texttt{Setup} \leftarrow (\kappa, DB)$: Taking as input a security parameter κ and an index database DB, it outputs the secret key sk, an encrypted dictionary EDX, and an encrypted multi-map EMM. The algorithm is run by the data owner (D).
- $(\Gamma) \leftarrow \texttt{Authorization token generation} \leftarrow (sk, W_{auth})$: Using as input the secret key sk and a vector of keywords $W_{auth} = (w_1, \cdots, w_q)$, for each keyword w_i in the vector, it creates a sub-token $\Gamma_i = (gtk_i, dtk_i, ltk_j)$ containing a global token gtk_i, a dictionary token dtk_i and for all keywords w_j, with $1 \leq j \leq q$ and $j \neq i$, a local token ltk_j. The algorithm is run by the data owner (D) and outputs authorization token $\Gamma = (\Gamma_1, ..., \Gamma_q)$.
- $(\gamma) \leftarrow \texttt{Search token generation} \leftarrow (\Gamma, \Delta)$: Using as input an authorization token Γ and a boolean query Δ, where Δ is a query written

in conjunctive normal form (CNF) as $\Delta_1 \wedge \cdots \wedge \Delta_l$, and where each $\Delta_i = w_{i,1} \vee \cdots \vee w_{i,q}$ is a disjunction, for the first disjunction Δ_1 it calculates the disjunction IEX sub-token γ_1 as follows:

- for each keyword $w_{1,j}$ in Δ_1 except the last, it creates the sub-token $\gamma_{1,j} = (gt\bar{k}_{1,j}, dt\bar{k}_{1,j}, lt\bar{k}_{k,j})$ containing the global token $gt\bar{k}_{1,j}$, the dictionary token $dt\bar{k}_{1,j}$ and for all keywords $w_{1,k}$, with $j+1 \leq k \leq q'$, the local token $lt\bar{k}_{k,j}$. Finally, for the last keyword $w_{1,q'}$ only the global token $gt\bar{k}_{1,q'}$ is kept and the output is the search token $\gamma_1 = (\gamma_{1,1} \cdots \gamma_{1,q'-1}, gt\bar{k}_{1,q'})$.

For every following disjunction $\Delta_i, 2 \leq i \leq l$ it computes the sub-token γ_i containing the local tokens between every keyword in Δ_1 and every keyword of Δ_i, as follows:

- for each keyword $w_{1,j}$ in Δ_1 it calculates the vector of local tokens $lt\bar{k}_{j,i} = (lt\bar{k}_{j,i,k}), 1 \leq k \leq q'$ between the keyword $w_{1,j}$ in the first disjunction and every keyword k in the i-th disjunction. Then the output is $\gamma_i = (lt\bar{k}_{1,i} \cdots lt\bar{k}_{q',i})$.

The algorithm is run by the search client (C) and the final output is a search token $\gamma = (\gamma_1, ..., \gamma_{q'})$.

- (T) $\mathtt{Search} \leftarrow (\mathsf{EDB}, \gamma)$: Using as input $\mathsf{EDB} = (\mathsf{EDX}, \mathsf{EMM})$ and a search token $\gamma = (\gamma_1, ..., \gamma_{q'})$, for the first search sub-token $\gamma_1 = (\gamma_{1,1} \cdots \gamma_{1,q'-1}, gt\bar{k}_{1,q'})$, the server performs the IEX search as follows:
  - For every element $\gamma_{1,i} = (gt\bar{k}_{1,i}, dt\bar{k}_{1,i}, lt\bar{k}_{k,i}), 1 \leq i \leq q'-1$:
    - First it uses $gt\bar{k}_{1,i}$ to query the global multi-map EMM, to recover the set $T_{1,i}$ of document identifiers containing w_i.
    - Then it uses $dt\bar{k}_{1,i}$ to query the encrypted dictionary EDX to recover the local multi-maps for w_i.
    - Finally, it uses the local tokens $lt\bar{k}_{k,i}$, with $i+1 \leq k \leq q'$ to query the local multi-maps, to recover the set of document identifiers T' that contain both w_i and w_k and removes them from $T_{1,i}$.
  - For the last element in γ_1, $gt\bar{k}_{1,q'}$, it recovers the document identifiers $T_{1,q'}$ containing $w_{q'}$.
  - Finally, the server calculates the set of document identifiers T_1, containing the document identifiers $T_{1,i}$ through $T_{1,q'}$.

  For every following search sub-token $\gamma_i = (lt\bar{k}_{1,i} \cdots lt\bar{k}_{q',i}), i \geq 2$, the server:
  - Uses $dt\bar{k}_{1,i}$ from γ_1 to query the encrypted dictionary EDX to recover the local multi-maps for w_i.
  - Then, it uses the local tokens $lt\bar{k}_{k,i}$, with $1 \leq k \leq q'$ to query the local multi-maps, to recover the set of document identifiers $T_{k,i}$ that contain both w_i and w_k.

- Then it calculates the union of all the common document identifiers $T_i = \bigcup_k T_{k,i}$
- and finally replaces T_1 with the intersection of T_i and T_1.

At the end, the server outputs the remaining set of identifiers in T_1, which is the resulting set of document identifiers for the query Δ.

The algorithm is run between the search client (C) and the storage and query server (S).

Note that the `Setup` and `Search` algorithms of the MC-SSE scheme are the same as the `Setup` and `Search` algorithms of the original BIEX scheme.

6.4 Security and Privacy Analysis

Our MC-SSE scheme is built over the BIEX scheme for which several SSE requirements have been proven. Based on the MC-SSE threat model presented in Section 6.2 and security and privacy requirements presented in Section 2.4, a security and privacy analysis is conducted below for each of the expected requirements:

Lemma 6.1. ***Index and document privacy****: S or any other entities are not able to deduce any sensitive information about the plaintext of the stored encrypted data, nor the associated keywords.*

Proof. The resulting encrypted data obtained thanks to the MC-SSE `Setup` algorithm are exactly the same as the ones generated by the BIEX `Setup` algorithm. As a consequence, our MC-SSE scheme inherits from the requirement Index and document privacy of the BIEX scheme. □

Lemma 6.2. ***Access pattern privacy****: S is not able to deduce any information about the data from the search results.*

Proof. The search results obtained thanks to the MC-SSE `Search` algorithm are exactly the same as the ones obtained from the BIEX `Search` algorithm. As a consequence, our MC-SSE scheme inherits from the requirement access pattern privacy of the BIEX scheme. □

Lemma 6.3. ***Query privacy****: S is not able to deduce the type of statistics being performed.*

Proof. The search method applied by S thanks to the MC-SSE `Search` algorithm is the exact same method with the BIEX `Search` algorithm. As a consequence, our MC-SSE scheme inherits from the requirement access pattern privacy of the BIEX scheme. However, S is unable to deduce the type of performed statistics, is able to deduce that a client is doing the exact same request if C is reusing the same authorization token for the exact same request to S. To mitigate that issue, C must be careful not to reuse any elements of the authorization token to S, or should ask for a new authorization token to D (cf. Section 6.3). □

Lemma 6.4. ***Query authorization****: Only authorized clients on authorized keywords only are able to extract statistics from S.*

Proof. Our original MC-SSE scheme does not prevent itself against any client stealing an authorization token or a search token and issuing an illegitimate request to S. However, the unauthorized usage of tokens can be prevented as follows. D can issue a certificate of ownership for the authorized client. This certificate signed by D can be computed over a signed randomized accumulator $Acc = g^{\prod_{a_{i,j} \in \Gamma} a_{i,j} \cdot ID_C}$, where g is a group of prime order q, $a_{i,j} \in Z_q$ are the elements of the authorization token $\Gamma = (dtk_i, gtk_i, ltk_j, gtk_q)$, and $ID_C \in Z_q$ is the ID of search client (C). C receiving the certificate is then able to extract his own search token and to adapt the accumulator by removing the elements selected for his search token γ : $Acc_C = g^{\prod_{a_{i,j} \in \Gamma \setminus \gamma} a_{i,j}}$, where $a_{i,j}$ are all the elements of the authorization token Γ, excluding the elements of the search token γ itself. S can check the validity of the certificate issued for C by computing $Acc_C^{\prod_{a_{i,j} \in \gamma} \cdot ID_C}$ and by checking that the signature is valid with regard to the resulting Acc_C. Moreover, the underlying authenticated channel enables S to detect spoofing and replay attacks over the pair - certificate and search token. □

Lemma 6.5. ***Privilege escalation prevention****: C is not able to collude with other clients to issue a valid search token over a superset of keywords which D did not authorize.*

Proof. Suppose two clients C_i and C_j with authorization tokens Γ_i authorizing keywords in vector $W_{auth_i} = (w_{i1}, \cdots, w_{iq})$ and Γ_j authorizing keywords in $W_{auth_j} = (w_{j1}, \cdots, w_{jq'})$, respectively ($w_{jk}$ are not elements of W_{auth_i}) try to collude to issue a new token for the superset of keywords authorized in Γ_i and Γ_j, to be able to perform cross-searches, i.e., queries combining keywords from the two disjoint authorization tokens. The resulting combined Γ_{ij} for the keywords in $W_{auth_{ij}} = (w_{i1}, \cdots, w_{iq}, w_{j1}, \cdots, w_{jq'})$ will not be usable to perform cross-searches, as although Γ_{ij} will contain the global tokens and dictionary tokens of all the combined keywords, it will not contain the local tokens for the combinations of keywords between the two authorization tokens. Therefore, authorization tokens could not be combined to authorize searches on combinations of keywords not already allowed by the initial authorization tokens, and the privilege escalation prevention is supported. □

Lemma 6.6. ***Data minimisation****: The transaction data items stored are reduced only to the necessary data items for service usage analysis.*

Proof. D needs to adequately select the set of keywords for limiting keywords to what is necessary for service usage analysis. The selection of keywords is a matter of regulation to respect and a matter of strategy for the company which needs relevant analysis results. □

6.5 Experimental results

The MC-SSE evaluation consisted of experiments with up to 1 M documents, containing synthetic parking transactions, resulting in 21 M document-keyword pairs. Experiments were conducted on both the original BIEX scheme and the MC-SSE scheme for the same dataset. The source code of the Clusion BIEX library is available online on the GitHub repository[9] and the source code for the multi-client extension of the Clusion BIEX library is available on the on the GitHub repository[10]. A docker container with the multi-client library extension bundled with a web application for testing its functionality is also available online on the Docker Hub repository[11]. Experiments were executed on the Grid'5000 testbed[12] with Intel Xeon Gold 6130 (Skylake, 2.10 GHz, 4 CPUs/node, 16 cores/CPU) processors and 60 GB of RAM, running Debian 11 (64-bit) OS. The experimental results confirm the correct functionality of the multi-client extension of the BIEX SSE scheme library. The performance evaluation of the MC-SSE library implementation shows that the properties of the original BIEX SSE scheme algorithm are retained, offering practical and efficient boolean search functionality.

In particular, as illustrated in Figure 13, the efficiency of the search functionality for MC-SSE is consistent with the original BIEX performance, taking approximately 3-30 ms, to perform a boolean search over 1 M documents (21 M document-id pairs). Note that the query expression includes 2 disjunctions (sub-queries) with 2 keywords each, of the form $((w \vee x) \wedge (y \vee z))$, with the search time depending on the selectivity of the first disjunction $((w \vee x))$ of the query, i.e., the number of documents returned by the first sub-query. The slightly smaller times in the MC-SSE search duration presented, mainly in higher values of the search times, is due to slight improvements in the Java code for the implementation of the search functions in the Clusion library.

In the multi-client version of the scheme, the main difference is the creation of the authorization token Γ, which includes a superset of all the sub-tokens for the included keywords, hence being larger in size compared to the equivalent BIEX search token. The experimental evaluation for the overhead introduced by the authorization token Γ consisted of creating authorization tokens and BIEX tokens for the same keywords and measuring the creation time and serialized size of the resulting tokens. For both types of tokens, the creation of tokens for keyword set sizes from $N \in [1, \cdots, 100]$ was evaluated, taking each time the N most frequent keywords in the dataset.

As illustrated in Figure 14, the creation of the authorization token Γ for the multi-client extension of BIEX, shows that the performance of the creation of the authorization token Γ displays the same general trend as the BIEX token creation, being exponential with the number of keywords in the token. Despite the creation time of the authorization token Γ being higher than the one of the

[9] `https://github.com/encryptedsystems/Clusion`
[10] `https://github.com/atasidou/MC-Clusion`
[11] `https://hub.docker.com/r/atasidou/multi-client_clusion`
[12] Grid'5000 testbed: https://www.grid5000.fr/

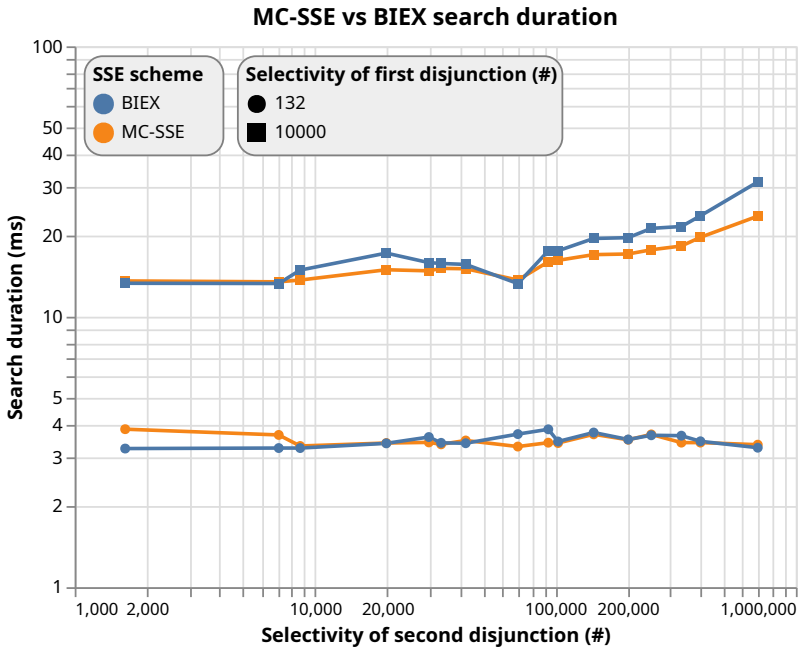

Figure 13: Boolean Search time.

BIEX token, it is just a constant factor higher and remains reasonable in absolute terms. The increased creation time is expected, as the authorization token Γ includes approximately double the elements compared to the corresponding BIEX token for the same keyword set, as illustrated in Figure 15.

7 Concluding remarks

In this paper, we present multidisciplinary work on a comprehensive privacy-preserving system. The work includes research areas starting from regulation compliance analysis, through the design of privacy-preserving parking registration and vehicle parking services to the deployment of privacy-preserving parking data processing features for data analysts. At the beginning of the article, we open up three research questions, namely **RQ1**, **RQ2**, and **RQ3**, which are discussed and addressed in the article.

First, we address the research question **RQ1:** What are the legal instruments, issues, and requirements for the deployment of such a system? To do so, we provide legal analysis for parking scenarios in compliance with current EU regulations and directives. From a legal point of view, it is obvious that the use of connected objects in cars requires a lot of precautions. While the legislation governing the processing of drivers' personal data (GDPR) is a cornerstone, ad-

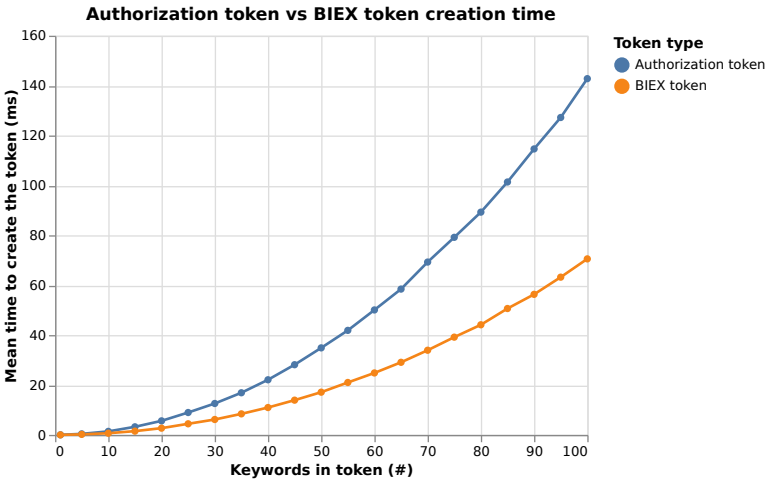

Figure 14: Token creation time.

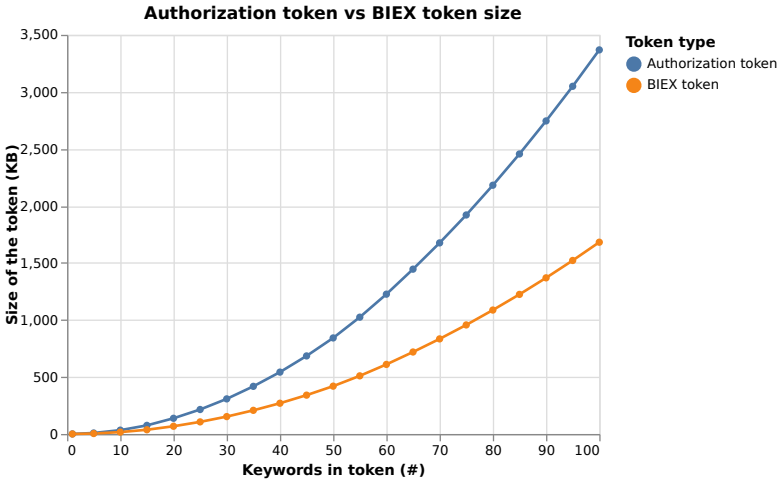

Figure 15: Token size.

ditional security obligations are enshrined in other European legislation. The key principle that drives the most privacy and security requirements is the privacy by design and by default obligation. This approach is accompanied by an appropriate security obligation regarding the risks incurred by users of the smart parking service. This scalable approach is completed by the ITS Directive. One has also to keep in mind that, depending on (1) the technical choices made for the implementation of the service and (2) the stakeholder involved, additional sectorial Regulations could apply. In particular, if a car manufacturer

is engaged in the development of the device/application used to provide the service, application of the EU Regulation on Vehicles General Safety Regulation and UNECE Regulation n155 could be triggered. In such cases, an additional layer of technical and cybersecurity requirements should be met to ensure legal compliance of a smart parking service. Finally, we would like to insist on the fact that an optimal security also requires the implementation of more overall organisational measures.

Second, we address the research question **RQ2:** How to build a privacy-preserving system which meets the requirements from RQ1? Which Privacy-Enhancing Technology (PET) can be used in order to protect users' privacy during using the system, i.e., reservation of parking slots and parking vehicle actions? Here, we base on privacy and security requirements identified from the legal analysis and we propose a novel privacy-preserving parking system. The system protects users' privacy and prevents tracking and profiling of users while using the system (i.e, during parking reservations and vehicle parking actions). On the other hand, the system allows revocation and de-anonymization of malicious users committing fraud. To do so, more system entities, namely PSP, PLT, and IDP, must collaborate. The cryptographic core of our system is built on provable secure PETs technologies such as group and blind signatures. We provide both security analysis of our system and experimental results.

Finally, we address the research question **RQ3:** How to allow third parties to perform statistical analyses on the parking transaction data, in a privacy preserving way? Which PET can be used to support this task? To do so, we deploy mechanisms for privacy-preserving data processing to our parking system. Completed parking transactions are stored in a dataset, containing only a subset of the data items concerning the transaction information, following the data minimization principle. Using a Searchable Symmetric Encryption (SSE) scheme, this dataset is outsourced to an external search service and stored as a searchable encrypted dataset. The existing efficient and secure BIEX SSE scheme [42], with high query expressiveness support is extended to the multi-client setting, to allow for authorized parties to perform searches on the encrypted dataset. In this manner, queries can be submitted to the search server to produce statistics on the parking system usage. A security analysis is provided for the proposed solution and experimental results show the applicability and efficiency of the system.

To our knowledge, our work in this paper is the first to consider both compliance to regulations (e.g., GDPR) and privacy protection for parking solutions. Most existing solutions mainly focus on some particular technological aspects such as route planning or autonomous parking. Our work is also very comprehensive by presenting both a technical design and an implementation to demonstrate its feasibility. From the figures in Section 5.4, it is clear that our parking solution is efficient enough to be deployed in practice.

Acknowledgments

This paper is partly supported in part by European Union's Horizon 2020 research and innovation program under grant agreement No 830892, project SPARTA, and in part by the Ministry of the Interior of the Czech Republic under grant VJ01030002. Author Florian Jacques has been partly supported by the project VIADUCT under the reference 7982 funded by Service Public de Wallonie (SPW), Belgium. The publication only reflects opinion of the authors. Experiments presented in Section 6 of this paper were carried out using the Grid'5000 testbed, supported by a scientific interest group hosted by Inria and including CNRS, RENATER and several Universities as well as other organizations (see https://www.grid5000.fr).

References

[1] Masayuki Abe and Tatsuaki Okamoto. "Provably secure partially blind signatures". In: *Annual International Cryptology Conference*. Springer. 2000, pp. 271–286.

[2] Wesam Al Amiri et al. "Privacy-preserving smart parking system using blockchain and private information retrieval". In: *2019 International Conference on Smart Applications, Communications and Networking (SmartNets)*. IEEE. 2019, pp. 1–6.

[3] Miguel E Andrés et al. "Geo-indistinguishability: Differential privacy for location-based systems". In: *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. 2013, pp. 901–914.

[4] O. Batura et al. "Artificial intelligence in road transport: annex to cost of non-Europe report". In: *European Union, Brussel* (2021), pp. 60–63.

[5] Hugh Beale. "Digital Content Directive And Rules For Contracts On Continuous Supply". In: *J. Intell. Prop. Info. Tech. & Elec. Com. L.* 12 (2021), p. 96.

[6] Mira Belenkiy et al. "Randomizable proofs and delegatable anonymous credentials". In: *Annual International Cryptology Conference*. Springer. 2009, pp. 108–125.

[7] Alex Biryukov and Sergei Tikhomirov. "Security and privacy of mobile wallet users in Bitcoin, Dash, Monero, and Zcash". In: *Pervasive and Mobile Computing* 59 (2019), p. 101030.

[8] O. Bittner et al. "The Forgotten Threat of Voltage Glitching: A Case Study on Nvidia Tegra X2 SoCs, https://arxiv.org/abs/2108.06131". In: *Fault Diagnosis and Tolerance in Cryptography* (2021).

[9] Dan Boneh and Xavier Boyen. "Short signatures without random oracles and the SDH assumption in bilinear groups". In: *Journal of cryptology* 21.2 (2008), pp. 149–177.

[10] Ricard Borges and Francesc Sebé. "An efficient privacy-preserving pay-by-phone system for regulated parking areas". In: *International Journal of Information Security* 20.5 (2021), pp. 715–727.

[11] Ricard Borges and Francesc Sebé. "Parking tickets for privacy-preserving pay-by-phone parking". In: *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society*. 2019, pp. 130–134.

[12] Jan Camenisch, Manu Drijvers, and Jan Hajny. "Scalable revocation scheme for anonymous credentials based on n-times unlinkable proofs". In: *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society*. 2016, pp. 123–133.

[13] Jan Camenisch and Markus Stadler. "Efficient group signature schemes for large groups". In: *Annual International Cryptology Conference*. Springer. 1997, pp. 410–424.

[14] J. M. Carvalho. "Sale of Goods and Supply of Digital Content and Digital Services – Overview of Directives 2019/770 and 2019/771". In: *Journal of European Consumer and Market Law* 8.5 (2019), pp. 194–201.

[15] Matthias Cäsar et al. "A survey on Bluetooth Low Energy security and privacy". In: *Comput. Networks* 205 (2022), p. 108712.

[16] Ioannis Chatzigiannakis, Andrea Vitaletti, and Apostolos Pyrgelis. "A privacy-preserving smart parking system using an IoT elliptic curve based security platform". In: *Computer Communications* 89 (2016), pp. 165–177.

[17] David Chaum. "Blind signatures for untraceable payments". In: *Advances in cryptology*. Springer. 1983, pp. 199–203.

[18] Roger Dingledine, Nick Mathewson, and Paul Syverson. *Tor: The second-generation onion router*. Tech. rep. Naval Research Lab Washington DC, 2004.

[19] Evan Duffield and Daniel Diaz. *Dash: A privacycentric cryptocurrency*. 2015.

[20] F. Dumortier. "La sécurité des traitements de données, les analyses d'impact et les violations de données". In: *Le règlement général sur la protection des données (RGPD/GDPR) – Analyse approfondie*. Ed. by C. de Terangne et K. Rosier. Larcier, 2018, pp. 234–240.

[21] Petr Dzurenda et al. "Privacy-Preserving Online Parking Based on Smart Contracts". In: *The 16th International Conference on Availability, Reliability and Security*. 2021, pp. 1–10.

[22] EC. *General Safety Regulation – Secondary Legislation*. 2021.

[23] EDPB. *Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications*. 2020. URL: `https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf`.

[24] EDPD. *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications)*. 2020.

[25] EDPD. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*. 2019.

[26] ENISA. *Cyber Security and Resilience of smart cars*. 2016.

[27] ENISA. *Recommendations for the Security of Connected and Automated Mobility*. 2021.

[28] EU. *Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC*. 2019.

[29] EU. *Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport*. 2010.

[30] EU. *Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services*. 2019.

[31] EU. *Regulation (EU) 2016/679 of the European Parlament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. 2016. URL: `https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679`.

[32] EU. *Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (Text with EEA relevance)*. 2019.

[33] Yunyi Fang et al. "Blockchain-based privacy-preserving valet parking for self-driving vehicles". In: *Transactions on Emerging Telecommunications Technologies* 32.4 (2021), e4239.

[34] Amos Fiat and Adi Shamir. "How to prove yourself: Practical solutions to identification and signature problems". In: *Conference on the theory and application of cryptographic techniques*. Springer. 1986, pp. 186–194.

[35] Qingqing Gan et al. "Dynamic Searchable Symmetric Encryption with Forward and Backward Privacy: A Survey". In: *Network and System Security*. Springer. 2019, pp. 37–52.

[36] Ricard Garra, Santi Martınez, and Francesc Sebé. "A privacy-preserving pay-by-phone parking system". In: *IEEE Transactions on vehicular technology* 66.7 (2016), pp. 5697–5706.

[37] F. Goldstein. "Understanding the UNECE WP.29 Cybersecurity Regulation (CSMS)". In: *https://upstream.auto/blog/understanding-the-unece-wp-29-cybersecurity-regulation/* (2020).

[38] Jan Hajny et al. "Anonymous Data Collection Scheme from Short Group Signatures." In: *ICETE (2)*. 2018, pp. 366–375.

[39] Jan Hajný et al. "Privacy ABCs: Now Ready for Your Wallets!" In: *Proceedings of The 19th International Conference on Pervasive Computing and Communications (IEEE PerCom 2021)*. Mar. 2021. Chap. 170757, pp. 686–691.

[40] Cheng Huang et al. "Secure Automated Valet Parking: A Privacy-Preserving Reservation Scheme for Autonomous Vehicles". In: *IEEE Transactions on Vehicular Technology* 67.11 (2018), pp. 11169–11180. DOI: 10.1109/TVT.2018.2870167.

[41] Seny Kamara. "Encrypted Search". In: *XRDS* 21.3 (Mar. 2015), pp. 30–34. ISSN: 1528-4972. DOI: 10.1145/2730908. URL: https://doi.org/10.1145/2730908.

[42] Seny Kamara and Tarik Moataz. "Boolean searchable symmetric encryption with worst-case sub-linear complexity". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2017, pp. 94–124.

[43] George Kappos et al. "An empirical analysis of anonymity in zcash". In: *27th {USENIX} Security Symposium ({USENIX} Security 18)*. 2018, pp. 463–477.

[44] Muhammad Khalid et al. "From smart parking towards autonomous valet parking: A survey, challenges and future Works". In: *Journal of Network and Computer Applications* 175 (2021), p. 102935.

[45] M. Knockaert et al. "Privacy-by-Design in Intelligent Infrastructures". In: *Deep diving into data protection: 1979-2019: celebrating 40 years of research on privacy data protection at the CRID*. Larcier, 2021, pp. 309–343.

[46] Zengpeng Li et al. "PriParkRec: Privacy-preserving decentralized parking recommendation service". In: *IEEE Transactions on Vehicular Technology* 70.5 (2021), pp. 4037–4050.

[47] Benoıt Libert and Damien Vergnaud. "Multi-use unidirectional proxy re-signatures". In: *Proceedings of the 15th ACM conference on Computer and communications security*. 2008, pp. 511–520.

[48] Michael M Losavio et al. "The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security". In: *Security and Privacy* 1.3 (2018), e23.

[49] Antoni Martınez-Ballesté, Pablo A Pérez-Martınez, and Agusti Solanas. "The pursuit of citizens' privacy: a privacy-aware smart city is possible". In: *IEEE Communications Magazine* 51.6 (2013), pp. 136–141.

[50] G Indra Navaroj and E Golden Julie. "Smart Parking in Smart Cities Using Secure IoT". In: *Research Anthology on Blockchain Technology in Business, Healthcare, Education, and Government*. IGI Global, 2021, pp. 1484–1507.

[51] Shen Noether. "Ring SIgnature Confidential Transactions for Monero." In: *IACR Cryptol. ePrint Arch.* 2015 (2015), p. 1098.

[52] Pascal Paillier. "Public-key cryptosystems based on composite degree residuosity classes". In: *International conference on the theory and applications of cryptographic techniques*. Springer. 1999, pp. 223–238.

[53] Aude Plateaux et al. "An e-payment architecture ensuring a high level of privacy protection". In: *International Conference on Security and Privacy in Communication Systems*. Springer. 2013, pp. 305–322.

[54] David Pointcheval and Olivier Sanders. "Short randomizable signatures". In: *Cryptographers' Track at the RSA Conference*. Springer. 2016, pp. 111–126.

[55] N. Purtova. "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law". In: *Law, Innovation and Technology* (2018), pp. 40–81.

[56] Sara Ricci et al. "Privacy-Enhancing Group Signcryption Scheme". In: *IEEE Access* 9 (2021), pp. 136529–136551.

[57] K. Sein. ""Goods With Digital Elements" and the Interplay With Directive 2019/771 on the Sale of Goods". In: *SSRN, (http://dx.doi.org/10.2139/ssrn.3600137)* (2020).

[58] Mitsunari Shigeo. *Mcl library*. `https://github.com/herumi/mcl`. 2018.

[59] Qiang Tang. "Another Look at Privacy-Preserving Automated Contact Tracing". In: *ACM Trans. Spatial Algorithms Syst.* 8.2 (2022), pp. 1–27.

[60] Fadi Al-Turjman and Arman Malekloo. "Smart parking in IoT-enabled cities: A survey". In: *Sustainable Cities and Society* 49 (2019), p. 101608.

[61] Fadi Al-Turjman, Hadi Zahmatkesh, and Ramiz Shahroze. "An overview of security and privacy in smart cities' IoT communications". In: *Transactions on Emerging Telecommunications Technologies* (2019), e3677.

[62] UNECE. *Proposals for Interpretation Documents for UN Regulation No. 155 (Cyber security and cyber security management system)*. ECE/TRANS/WP.29/2021/59. 2021.

[63] UNECE. *UN Regulation No 155 – Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system*. 2020.

[64] Upstream. *Global Automative Cybersecurity Report - Automotive Cyber Threat Landscape in Light of New Regulations*. 2022.

[65] Upstream. *Global Automative Cybersecurity Report, Research into Cyber Attack Trends in Light of Cybersecurity Standards and Regulations*. 2021.

[66] Mario Weber and Ivana Podnar Žarko. "A regulatory view on smart city services". In: *Sensors* 19.2 (2019), p. 415.

[67] Liehuang Zhu et al. "ASAP: An anonymous smart-parking and payment scheme in vehicular networks". In: *IEEE Transactions on Dependable and Secure Computing* 17.4 (2018), pp. 703–715.