Decentralized Privacy-preserving Access for Low Emission Zones

Carles Anglès-Tafalla[1], Sara Ricci[2], Petr Dzurenda[2],
Jan Hajny[2], Jordi Castellà-Roca[1] and Alexandre Viejo[1]
[1]*UNESCO Chair in Data Privacy, Department of Computer Science and Mathematics, Rovira i Virgili University, Av. Països Catalans 26, Tarragona, Spain*
[2]*Department of Telecommunications, Brno University of Technology, Technicka 12, Brno, Czech Republic*

Keywords: Low Emission Zones, Smart Cities, Privacy, Anonymity, Group Signatures, Smart Contracts.

Abstract: Low Emission Zones (*LEZ*) are a common mechanism to regulate traffic jams and environmental pollution. Nevertheless, the problems of this solution are lack of privacy its reliance on centralized entities. The presented scheme continues the emerging trend of using cameras to only identify dishonest users, and proposes a decentralized access control system for LEZs, which, through a tailored group signature model, addresses the user's privacy requirements that a public ledger like blockchain demands.

1 INTRODUCTION

The registered high levels of environmental pollution, due in large part to urban traffic jams, has become a serious problem for large cities all around the world. The implementation of LEZ, i.e. areas where restrictions or surcharges are applied to drivers in accordance with their vehicles' emissions, is one of the measures that proliferated the most to address this problematic. Sweden, Italy, United Kingdom and Germany are examples in which LEZs are applied [1].

Currently deployed automated systems for LEZs are based on camera networks, like London's scheme[1], whose purpose is to indiscriminately take photographs of vehicles' license plates to verify if the vehicle's owner is paying the corresponding vehicle emission category fee. Systems with an intrusive nature as the aforementioned ones fuelled the appearance of more privacy-friendly approaches. These proposals are mainly focused on gathering anonymous location proofs, generated when vehicles meet access infrastructures, for, later, determining and charging the corresponding fees. This way of proceeding, however, poses a strong dependence on the centralized entities who control the system infrastructures, acknowledge the generated poofs and compute its corresponding fees.

Recent decentralized protocols, built on blockchain technology, can be applied to settle transactions between vehicles and LEZ infrastructures without the involvement of trusted third parties, putting an end to the favorable position these centralized entities hold. Nevertheless, the use of a public ledger brings new privacy challenges to the field, as published transactions fall into the public domain and, thus, any contained driver information should be accordingly protected.

In the light of the identified issues, in this work, we follow the privacy-focused emerging trend of avoiding the indiscriminate record of all vehicles' license plates in pursuit of designing a new decentralized access control system for LEZ. The cornerstone of this scheme is to pursue the decentralization the blockchain paradigm poses, while providing, through a tailored group signature scheme, the user privacy requirements that the use of a public ledger requires.

1.1 Related Work

Initial access control systems for LEZs (Balasch et al., 2010; Chen et al., 2012; Garcia et al., 2013) relied on the use of an On-Board-Unit (OBU) for gathering fee-relevant data; a centralized third party, i.e. Service Provider (SP), acknowledging the whole process and charging the required fee; and a camera-based checkpoint network recording vehicles license plates to avoid users' fraud.

In the recent years, a new paradigm has taken hold since it was proposed in (Jardí-Cedó et al., 2018) and followed by (Jardí-Cedó et al., 2016; Anglès-Tafalla

[1]Urban Access Regulations In Europe deployment map, http://urbanaccessregulations.eu/userhome/map

Anglès-Tafalla, C., Ricci, S., Dzurenda, P., Hajny, J., Castellà-Roca, J. and Viejo, A.
Decentralized Privacy-preserving Access for Low Emission Zones.
DOI: 10.5220/0007953504850491
In *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications (ICETE 2019)*, pages 485-491
ISBN: 978-989-758-378-0

et al., 2018; Hoffmann et al., 2018). This new model promotes that users' anonymity is always preserved unless they try to commit fraud. In this matter, such systems only take photos of vehicle's license plates in case the authentication process with the system infrastructures is not completed or totally omitted. During authentication those systems protect users' privacy through different mechanisms such as group signatures, pseudonyms or zero knowledge proofs. Despite of their privacy-preserving mechanisms, every one of the previous works rely on a centralized entity, usually a SP, to acknowledge vehicles' access data and ascertain their traffic fee inside the LEZ.

In order to shed the dominant position these centralized entities hold, a decentralized approach based on smart contracts, which price and pay vehicles' access dealing them as blockchain transactions, is presented in (Anglès-Tafalla et al., 2019). Building on top of previous works, its privacy scheme is based on pseudonyms for the sake of a lightweight access phase. Although this work successfully tackles the centralization issues found in the literature regarding the LEZ access control systems, the use of pseudonyms in a public ledger, like a blockchain, entails relevant threats in terms of user's traceability and likability. In that way, the privacy-preserving strength of this scheme mostly relies on its pseudonym renewal policy, whose regeneration decision in the end falls on the client-side and, hence, on the users' criteria.

1.2 Contribution and Plan of this Paper

Bearing in mind the privacy issues found in the literature, our scheme proposes a new decentralized privacy-preserving access control system for LEZ*s* in which user's anonymity is achieved through a tailored group signature scheme, outstanding for its lightweight signature process and not requiring key regeneration to preserve unlinkability. Under this premise, our approach allows treating LEZ accesses as transactions and decentrally settle them, by means of smart contracts, without the involvement of trusted third parties.

On that basis, users generate access evidences, signed on behalf of their vehicle emission category group, without disclosing their identities or permitting linkage between them. This is achieved even if these evidences are published in a public ledger like a blockchain. With this privacy-preserving scheme, user's anonymity is truly preserved without the need of client-on-demand credentials renewal process, which, due to their computational load, can interfere with critical real-time phases of the protocol.

In a nutshell, our proposal's contribution includes:

- *Revocable Anonymity:* the proposed system always preserves users' privacy as long as they follow the defined protocol, failing which their identities could be disclosed and their privacy revoked.
- *Decentralized System:* the system seizes the favorable position that centralized third parties, responsible of acknowledging access data and charging fees, have over users in favor of the decentralized model that blockchain and smart contracts pose.
- *Privacy-enhancing Signatures:* the system provides real privacy and unlinkability to users by means of a tailored group signatures scheme, without requiring credentials regeneration to achieve that.
- *Honest-user-friendly Fraud Control System:* the system is able to identify dishonest users, who alter or skip the protocol to commit fraud, without this process affecting the privacy of honest ones.

The remainder of this paper is organized as follows. Section 2 introduces the new proposal. Section 3 thoroughly details the protocol steps. Section 4 presents an evaluation of the proposed scheme. Finally, Section 5 reports some concluding remarks.

2 MODEL OF THE SYSTEM

Figure 1 shows a general overview of the protocol's steps, along with their actors, related to the access control scenario and its posterior payment phase. In this layout, the involved actors, i.e. Drivers (D) and Access control infrastructure (AC), should obtain valid credentials from the LEZ Administrator (LA) in order to securely interact with other entities of the system. In case of D, the vehicle's OBU should obtain group signature credentials bound to its vehicle emissions category in order to certify this condition to the AC. Furthermore, all entities interacting with the smart contract, i.e. D, AC and LA, should generate digital wallets for that purpose.

The access scheme starts when D approaches to the LEZ entrance and her OBU automatically initiates the protocol. The detection of *Bluetooth Low Energy* beacons can be, for instance, the trigger to automatize this process without D's intervention. On that awakening signal, D's OBU establishes a secure connection using a short-range communication system with the AC and, through an authentication process, proves the vehicle's emissions category that D is driving.

By successfully concluding this process, AC and D can agree an access receipt, containing the entrance

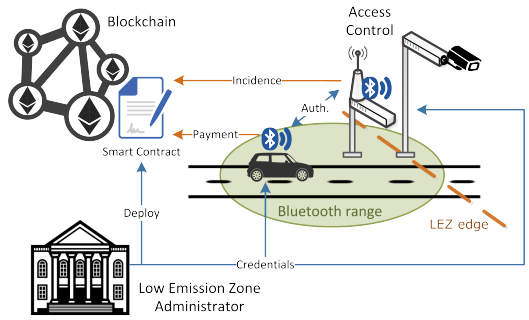

Figure 1: System's general overview.

parameters, which act as proof of their interaction. During the whole process D's privacy is preserved as all generated evidences are signed, due to our group signature scheme, on behalf of her vehicle's emissions category group. In this way, AC*s* are prevented from binding D's accesses. Conversely, if the process fails due to D's dishonest behavior, i.e. she tries to alter the protocol, AC will take a photo of D's license plate and, thus, disclosing the driver's identity.

Once a valid access receipt is obtained, D can initiate the payment process by interacting with the LA-deployed smart contract. For this, D remotely calls the payment function of the smart contract, sending the agreed access data as parameters. On the basis of this information, the smart contract's logic verifies its validity and calculates the fee to pay according to the last uploaded prices in the blockchain. If the access receipt is valid and it was issued by an LA-authorized AC, the corresponding amount of LEZ digital tokens is transferred from D's to AC's digital wallet.

When enough time elapsed for the access transaction being validated and added to the blockchain, the involved AC verifies the transaction's status to determine if the access payment was correctly conducted. In case any irregularity is found, e.g. the access transaction in not in the blockchain or its status is not set as "paid", AC interacts with the smart contract to publish an access incidence. In this process, the AC uploads to the blockchain its own access receipt copy, which also contains D's group signature. With this information published, the LA, as the groups manager, can disclose D's identity and, thus, revoke her privacy.

2.1 Blockchain Integration

The principle behind Blockchaint consists in granting equal decentralized trust to any node with the power of solving computational challenges, known as proof-of-work, and using it as a way to reach consensus. This concept was extended in (Wood, 2014) with Ethereum, whereby programmable logic programs, referred to as smart contracts, are executed on the Blockchain permitting to decentrally settle transactions of arbitrary resources.

The presented proposal uses Ethereum's smart contracts to include LEZ access data in blockchain transactions and automatically transfer its corresponding fee in terms of digital tokens. With this procedure, the nodes of the blockchain network are able to decentrally validate the vehicle access, allowing the omission of overseeing centralized third parties. The blockchain paradigm requires that network nodes, i.e., miners, contribute with their computational resources to validate transactions and further a trustworthy advancement of the chain. The miners of the proposed scenario would be: i) LA, which is the provider of digital tokens; and ii) ACs, which get monetary compensation for their participation in the system.

2.2 Group Signatures Integration

Group signature (Chaum and Van Heyst, 1991) allows the sender to anonymously sign a message on behalf of the group and, therefore, a receiver to verify that it is a valid signature without disclosing sender's identity. In other words, this approach provides data authenticity without disclosing the users' identity. Moreover, it is possible to revoke malicious users, i.e. the signature can be "opened" in case of fraud.

In (Hajny et al., 2018), we propose a novel group signature scheme based on Weak Boneh-Boyen (wBB) signature (Boneh and Boyen, 2008) and the efficient proofs of knowledge (Camenisch et al., 2016). This scheme has fast signature generation and provides all privacy-enhancing signature features, i.e. anonymity, unlinkability and untraceability. The wBB signatures were proven existentially unforgeable against a weak (non-adaptive) chosen message attack under the p-SDH assumption (Boneh and Boyen, 2008). The present article uses the proposed signature (Hajny et al., 2018) in order to add all the aforementioned features to the LEZ scheme.

3 PROTOCOL

Our system involves the four following actors: i) LEZ Administration (*LA*); ii) Drivers (*D*); iii) Access Control Infrastructure (*AC*); and iv) Cryptocurrency Mixing Service (*M*).

LA is the entity who is in charge of managing the LEZ and establishing the restrictions applied to the vehicles accessing this area. Among its tasks is to issue valid certificates to other system's entities and

deploy the LEZ's smart contract. *D*s are the potential users of the LEZ, who interact with the system's infrastructures through the on-board units (*OBU*) embedded in their vehicles. OBU*s* are devices able to perform cryptographic operations, equipped with GPS technology, 4G, Bluetooth and a tamper-proof Secure Element (*SE*). It is assumed that SE already has the vehicle's license plate stored in it. *AC*s are the infrastructures controlling the vehicle access to the LEZ. They are expected to be equipped with a camera, GPS, Bluetooth and internet access. *AC*s may be under control of one or more for-profit entities as long as the LA is not one of them. Finally, *M* is an independent entity in charge of obfuscate the tractability of blockchain transactions, so that transferred funds cannot be trailed back to the source digital wallet.

This section formalizes the different phases that drive the proposed system, giving enough detail to allow their implementation. These are: *On-board unit set-up*, *Wallet filling*, *Access* and *Payment*.

3.1 On-board Unit Set-up

The first step the users should fulfill is registering into the system and obtaining the adequate credentials to successfully interact with AC*s*. To this end, D's OBU establishes a secure communication channel, with the LA server and provides the vehicle data (plate number, car maker, model, etc.). The LA, as a governmental entity, is able to verify the correctness of these data and obtain the information of the vehicle's owner. Then, LA generates a 128-bit vehicle code *vc* and sends it as a One-Time-Secret (OTS) URL linked to D through a side channel (email, phone, etc.). D, once *vc* is retrieved, generates a key pair (sk_D, pk_D), a certificate signing request $CSR(pk_D)$, containing *vc*, and sends this last one back to LA. On the basis of $CSR(pk_D)$, LA verifies the validity of *vc* and issues its corresponding certificate $Cert(pk_D)$, including *vc* in the *CommonName* field and the vehicle emissions category *cat* as an extension. Finally, D checks the validity of the received certificate $Cert(pk_D)$ and stores the generated credentials.

Through the completion of the previous process, D obtains a valid LA-issued certificate $Cert(pk_D)$, which allows her to complete strong bilateral authentication with the other entities of the system. On this basis, D then establishes secure communication with LA, which comprises a two-way authentication. By means of this channel, LA and D are negotiating the group signature keys that D is using to validate her accesses. Figure 2 illustrates these steps.

D initiates the process preparing a key generation request *gr* which contains a random identifier id_D and

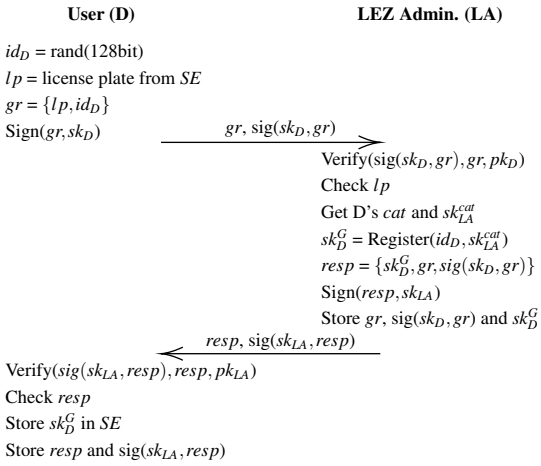

Figure 2: Group signature keys negotiation.

a license plate proof lp, generated by SE. D signs this request with her private key Sign(gr, sk_D) before sending it to LA. When LA receives a request *gr* from D, first, verifies its signature. If it is correct, checks the validity of the license plate lp and verifies if it matches the vehicle behind the code *vc* contained in D's certificate $Cert(pk_D)$. Then, selects the group private key sk_{LA}^{cat} associated with vehicle's emissions category and initiates the generation process. In this operation, LA, inputs sk_{LA}^{cat} and id_D to generate D's group private key sk_D^G. Detailed steps of *Register* process are defined in (Hajny et al., 2018). Finally, a generation response *resp*, containing the generated key and the D's generation request, along with its signature is sent back to D. In the other end, D verifies the response and stores all received data as proof of the generation process. sk_D^G is then stored in the SE of the OBU.

Once the credentials generation process is completed, D generates a group of Ethereum digital wallets $W_D^1..W_D^n$, as she is required to publish transactions on the blockchain for paying her LEZ access through the use of smart contracts. For this purpose, D generates a 256-bit private key sk_D^W, a 512-bit public key pk_D^W and its corresponding address, according to Ethereum key specs, for each wallet she is creating.

3.2 Wallet Filling

As the presented scheme contemplates the access fee payment with smart contracts, D*s* should purchase LEZ tokens, i.e. elements acting as native currency in our system, for their monetary transactions. For this purpose, it is expected that LA hosts a specific Internet portal where users can buy tokens in exchange of money or cryptocurrencies. In this matter, tokens purchased via cryptocurrency are expected to be anonymous, contrary to classic payment mechanisms, e.g.

credit card, which pose privacy threats for users.

In order to tackle this problem, D creates a temporal wallet W_D^T in which the purchased LEZ tokens will be transferred once bought from LA web portal. Then, D asks the cryptocurrency mixing service (e.g., ETH-Mixer[2]) to transfer the funds from W_D^T to her group of wallets $W_D^1..W_D^n$. M, by means of the mixing process, obscures the link generated between the source and destination wallets when funds are transferred, preventing the LA from linking the token purchaser with her transactions on the blockchain.

Furthermore, in order to avoid the linking of transactions that a wallet is involved in, D distributes her funds in small different amounts among several one-use wallets. In this way, D fractionally pays her access to the LEZ using different wallets and disposing the already-used empty ones in the process. Note that this process requires some planning by the client device when distributing D's token funds among all her wallets, as it should be able to combine them to add up the charging required fee.

3.3 Access

When D is accessing the LEZ, she establishes communication with AC and agrees the entrance parameters. When D reaches AC's communication range, both entities establish secure communication, via TLS, implying one-way authentication from AC; and perform the steps in Figure 3.

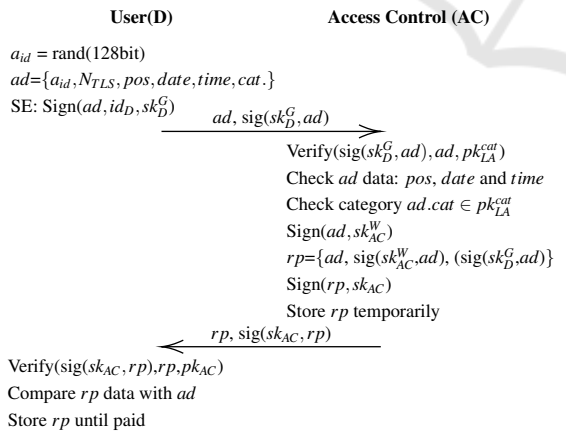

Figure 3: Access protocol.

D starts the process by sending the access data ad, including her position, date, time, vehicle emission category, a random access id a_{id} and a AC-generated nonce N_{TLS} from the previous TLS handshake. This data is signed, by the OBU's SE, on behalf of D's emission category group. On receipt of ad, AC verifies the correctness of the data and its signature by means of the corresponding group public key pk_{LA}^{cat}. If verifications are correct, AC prepares an access receipt, which consists in the received data ad signed using AC's digital wallet private key sk_{AC}^W, so it can be verified on-chain by the LEZ smart contract. This signature is sent back to D along with the original received message, i.e. ad and its D's group signature, signed with AC's private key sk_{AC} as a proof of their access agreement. D temporally stores this proof once she contrasted the received data rp with the sent one ad and verified both AC's signatures. The exact steps of signature generation and verification processes are detailed in (Hajny et al., 2018). If at some point D fails to complete this process by deliberately skipping or altering the protocol execution, the AC will take a photo of the vehicle's license plate. This photo will serve to identify the unauthenticated vehicle and, thus, revoke D's privacy.

3.4 Payment

Once the access parameters are agreed and D obtained an access receipt rp from AC, the user starts the payment process. LA, as the smart contract's owner, has the authority to update the prices list the smart contract inquires to determine the access fees. To do so, the LA calls the smart contract's method *set_prices* which uploads new prices to the blockchain.

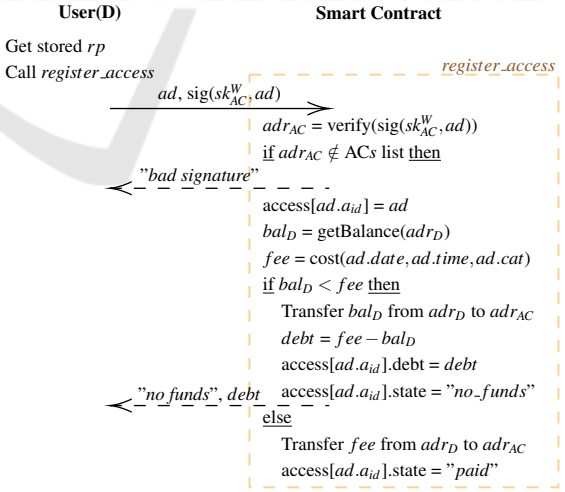

Figure 4: Payment protocol: Payment.

This process, shown, step by step, in Figure 4, starts when D interacts with the smart contract by invoking the *register_access* method. On this process, D upload as parameters the access data ad and AC's digital wallet signature sig(sk_{AC}^W,ad) contained in the access receipt rp received from AC. The smart con-

[2]ETH-Mixer, https://eth-mixer.com/

tract, for its part, verifies on-chain the validity of AC's signature, as its signed using Ethereum protocol standards, and if its issuer is a valid AC registered in the smart contract. Then, on the basis of date, time and vehicle category, the access fee is calculated according to the last registered prices and the corresponding amount is transferred from D's to AC's wallets in terms of LEZ tokens. In case of insufficient funds, the remaining amount is set as debt, so D can settle it using other wallets. Depending on the method outcome, access a_{id} status will be set a "bad signature", "no funds" or "paid". Once the status is set as "paid", no further action can be taken on this a_{id} access.

Once enough time elapsed for the access transaction being validated, AC verifies if a transaction a_{id} is published to the blockchain with "*paid*" status. In case these conditions are not met, AC publishes an incidence to the blockchain calling the *open_incidence* method. D's access data and its signature on behalf of her vehicle emission category group are sent as parameters. The smart contract, on its part, verifies if the conditions to open an incidence are met and publish D's group signature if required. LA, as smart contract's owner, is in charge of setting the elapsed time for an incidence to be opened. With this procedure, LA has the means to identify D through her group signature and initiate sanctioning measures against her.

Finally, it is assumed that LA, at each billing period, will monetarily reward AC*s*, in accordance to the gathered token amount, thereby getting profit from their services.

4 EXPERIMENTAL RESULTS

In this section, we evaluate the performance of protocol's phases whose feasibility is bound to strict temporal constraints. In a LEZs scenario, these restrictions are present between AC and D interaction during the Access phase, as vehicles have to finish this process while they are in range to communicate.

In order to perform this evaluation, we implemented the protocol steps described in Section 3.3 along with entities involved in the process: *D* and *AC*. The AC side is implemented in Java7 an run on a Raspberry Pi 2 using Raspbian OS. On the client side, D's OBU is impersonated by an Android application written in Java8 running on LG Nexus 5X and Android 6.0 OS. Finally, the OBU's SE is implemented in a ML4 smartcard 2KB RAM using Multos 4.1 OS and programmed in C. In this testbed, D's group signatures are performed using d224-sized elliptic curves. The rest of signatures and encryptions are computed using 2048-bits RSA scheme.

In order to support our evaluation and to provide a fair comparison, we implemented the Access phase of similar approaches in the literature (Jardí-Cedó et al., 2018; Jardí-Cedó et al., 2016; Anglès-Tafalla et al., 2019) and run tests under the same configuration.

4.1 Performance

As seen in Table 1, our protocol consumes in computation an average time of 1.038 seconds. More specifically, AC, who performs the most computational expensive operations, takes 0.594 seconds. Most of this time, 0.268, is spent in RSA signature generation, followed by group signature verification process, which comprises costly bilinear pairing operations, with 0.234 seconds. The remaining 0.092 seconds are spent in generating AC's digital wallet signature and other non-cryptographic operations. In this way, the driver's side is more lightweight and almost all 0.444 seconds are spent by the SE, which has lower computational power, for generating D's group signature. Putting that into perspective, this same process in AC's side will only take 0.053 seconds.

Table 1: Computation time comparison in seconds.

	Client side	AC side	Total
(Anglès-Tafalla et al., 2019)	.083	.367	.450
Our scheme	.444	.594	1.038
(Jardí-Cedó et al., 2018)	1.321	.582	1.903
(Jardí-Cedó et al., 2016)	1.339	.662	2.001

Our proposal is especially suited for LEZs scenarios, as stands for being lightweight on the client-side, which is composed by an OBU and its SE, and performing the most expensive operations on AC's side, which can be embedded with greater CPUs.

4.2 Comparison

Table 1 shows the access phase average times dedicated to computational tasks by most similar schemes in the literature. As can be seen, (Anglès-Tafalla et al., 2019) is, with difference, the most lightweight protocol. However, it does not contemplate the use of a SE on the client side, which results in fast RSA signature generations, and bases users' privacy protection on pseudonyms, which reduces signature verification complexity at the expense of users' linkability. Regarding the other group signature based approaches, (Jardí-Cedó et al., 2018; Jardí-Cedó et al., 2016), it draws special attention the times to complete their client computation. This is mainly caused because their clients are using 2048-bit RSA signatures that, due their scheme design, can only be generated by

the SE, posing the heaviest computational part on the slowest component.

Regarding our scheme, it achieves better times than the other group-signature schemes (Jardí-Cedó et al., 2018; Jardí-Cedó et al., 2016) due to a more lightweight client protocol. In that way, costly pairing operations are performed during group-signature verification and, thus, executed on the AC-side. This allows a light signature process on the client-side that proves feasible even if executed in the OBU's SE.

Finally, it also should be bore in mind that in (Anglès-Tafalla et al., 2019; Jardí-Cedó et al., 2018; Jardí-Cedó et al., 2016) a credential renewal process is needed to keep preserving the users' privacy and, until this new certificates are not generated, their LEZ accesses are linkable. In case of (Jardí-Cedó et al., 2018; Jardí-Cedó et al., 2016) this process can take up to 10 seconds as should be computed inside the SE.

In a nutshell, it can be stated that our system is more lightweight than other group-signature-based works, and can even compete with faster less privacy-preserving approaches based on pseudonyms. Furthermore, it fully provides unlikabilty and non-traceability without needing to regenerate, after each access, the drivers' credentials for achieving it.

5 CONCLUDING REMARKS

The access control system for LEZ we proposed in this article follows the recent decentralized trend of omitting third parties from access data acknowledgment and payment related processes in favor of blockchain and smart contracts technologies. Unlike other approaches, our system truly preserves the anonymity, non-traceability and unlikablility of honest users, through an efficient tailored group signature scheme, without the need of a client-on-demand credential renewal process to achieve it. On top of that, experimental results show that our system is more lightweight than similar group-signature-based LEZ access control systems in the literature.

ACKNOWLEDGMENTS

This work was supported by Government of Catalonia (grant SGR2017-705), the Spanish Government under SmartGlacis (TIN2014-57364-C2-R) and CONSENT (RTI2018-095094-B-C21), the Technology Agency of the Czech Republic under "Legal and technical tools for privacy protection in cyberspace" project (TL02000398) and European Union, Ministry of Education, Youth and Sports, Czech Republic and Brno, University of Technology under international mobility project MeMoV (CZ.02.2.69/0.0/0.0/16_027/00083710). The authors' opinion in this work are their own and do not commit UNESCO Chair in Data Privacy.

REFERENCES

Anglès-Tafalla, C., Castellà-Roca, J., Mut-Puigserver, M., Payeras-Capellà, M. M., and Viejo, A. (2018). Secure and privacy-preserving lightweight access control system for low emission zones. *Computer Networks*, 145:13–26.

Anglès-Tafalla, C., Castellà-Roca, J., and Viejo, A. (2019). Privacy-preserving and secure decentralized access control system for low emission zones. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops*. IEEE.

Balasch, J., Rial, A., Troncoso, C., Preneel, B., Verbauwhede, I., and Geuens, C. (2010). Pretp: Privacy-preserving electronic toll pricing. In *USENIX Security Symposium*, volume 10, pages 63–78.

Boneh, D. and Boyen, X. (2008). Short signatures without random oracles and the sdh assumption in bilinear groups. *Journal of Cryptology*, 21(2):149–177.

Camenisch, J., Drijvers, M., and Hajny, J. (2016). 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*, pages 123–133. ACM.

Chaum, D. and Van Heyst, E. (1991). Group signatures. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 257–265. Springer.

Chen, X., Lenzini, G., Mauw, S., and Pang, J. (2012). A group signature based electronic toll pricing system. In *2012 Seventh International Conference on Availability, Reliability and Security*, pages 85–93. IEEE.

Garcia, F. D., Verheul, E. R., and Jacobs, B. (2013). Cell-based privacy-friendly roadpricing. *Computers & Mathematics with Applications*, 65(5):774–785.

Hajny, J., Dzurenda, P., and Ricci, S. (2018). Anonymous data collection scheme from short group signatures. In *In SECRYPT 2018 Proceedings*, pages 1–10.

Hoffmann, M., Fetzer, V., Nagel, M., Rupp, A., and Schwerdt, R. (2018). P4TC - provably-secure yet practical privacy-preserving toll collection. *IACR Cryptology ePrint Archive*, 2018:1106.

Jardí-Cedó, R., Castellà, J., and Viejo, A. (2016). Privacy-preserving electronic road pricing system for low emission zones with dynamic pricing. *Security and Communication Networks*, 9:3197–3218.

Jardí-Cedó, R., Mut-Puigserver, M., Payeras, M. M., Castella-Roca, J., and Viejo, A. (2018). Time-based low emission zones preserving drivers' privacy. *Future Generation Computer Systems*, 80:558–571.

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151:1–32.