DRAFT

On Locational Privacy in the Absence of Anonymous Payments

Tilman Frosch, Sven Schäge, Martin Goll, Thorsten Holz

Horst Görtz Institute for IT Security, Ruhr-Universität Bochum, Germany

Abstract. In this paper we deal with the situation that in certain contexts vendors have no incentive to implement anonymous payments or that existing regulation prevents complete customer anonymity. While the paper discusses the problem also in a general fashion, we use the recharging of electric vehicles using public charging infrastructure as a working example. Here, customers leave rather detailed movement trails, as they authenticate to charge and the whole process is post-paid, i.e., are billed after consumption. In an attempt to enforce transparency and give customers the information necessary to dispute a bill they deem inaccurate, Germany and other European countries require to retain the ID of the energy meter used in each charging process. Similar information is also retained in other applications, where Point of Sales terminals are used. While this happens in the customers' best interest, this information is a location bound token, which compromises customers' locational privacy and thus allows for the creation of rather detailed movement profiles. We adapt a carefully chosen group signature scheme to match these legal requirements and show how modern cryptographic methods can reunite the, in this case, conflicting requirements of transparency on the one hand and locational privacy on the other. In our solution, the user's identity is explicitly known during a transaction, yet the user's *location* is concealed, effectively hindering the creation of a movement profile based on financial transactions.

1 Introduction

Blumberg and Eckersley define locational privacy as "the ability of an individual to move in public space with the expectation that under normal circumstances their location will not be systematically and secretly recorded for later use".[1] In a world of Big Data, where any fact about an individual's life, once revealed, will potentially be stored indefinitely, it is important to limit the data that is created or revealed in the first place. While completely anonymous systems would be desirable in many cases from a customer's side, legitimate business interests on the side of the vendor may prevent the adoption of a technical solution that relies on complete anonymity. In the context of financial transactions, the prevalent academic approach to protecting a user's locational privacy is to protect the user's *identity* and thus indirectly conceal their location. Various anonymous electronic cash (e-cash) schemes have been published[2] since Chaum published his seminal paper *Blind Signatures for Untraceable Payments*[3] in 1982. However, none has been (widely) adopted. Besides posing technical hurdles, e-cash often makes it hard for the vendor to walk the established path of resolving a dispute with a customer on front of a court of law, as the customer is not known – although many schemes reveal the customer's identity in case of double spending, but only then. Anonymous payment schemes also forfeit the option of post-paid good and services, where the customer needs to be billed and thus is typically known. Finally, there may be applications where regulations and legal restrictions prohibit the customer from being anonymous. Vendors in this market will be unable to provide anonymous payment services to their customers.

Under the premise that the customer must be identifiable, we thus must conceptionally deviate from the widespread paradigm of anonymizing customers in privacy-enhancing payment and billing

---

[1] Andrew J. Blumberg and Peter Eckersley, *On Locational Privacy, and How to Avoid Losing it Forever*, technical report (Electronic Frontier Foundation, 2009), accessed February 4, 2013, https://www.eff.org/wp/locational-privacy.

[2] E.g. David Chaum, "Security without identification: transaction systems to make big brother obsolete," *Commun. ACM* 28, no. 10 (October 1985): 1030-1044, issn: 0001-0782, doi:10.1145/4372.4373, http://doi.acm.org/10.1145/4372.4373;
David Chaum, Amos Fiat, and Moni Naor, "Untraceable Electronic Cash" in *Advances in Cryptology - CRYPTO* (1988); Stefan Brands, "Electronic cash systems based on the representation problem in groups of prime order" in *CRYPTO* (1993); Jan L. Camenisch, Jean-Marc Piveteau, and Markus A. Stadler, "An efficient electronic payment system protecting privacy," in *ESORICS* (1994).

[3] David Chaum, "Blind Signatures for Untraceable Payments," in A*dvances in Cryptology: Proceedings of CRYPTO '82* (1982).

systems. Instead of obscuring or removing identity information, in our solution, the user's identity is explicitly known during a transaction, yet the user's *location* is concealed. Our approach effectively hinders the creation of a movement profile based on financial transactions. We use the increasingly relevant example of re-charging electric vehicles and paying for energy on the go to showcase our approach. We do not exclude the possibility that our approach can be adapted to other settings that require the customer to be known during such a transaction.

Why Electric Vehicles? The electric vehicle (EV) scenario offers several interesting constraints. First of all, the proliferation of vehicles and infrastructure is limited, but rapidly increasing. Market research predicts up to 3.4 million annual world-wide sales of plug-in hybrid (PHEV) and battery electric vehicles (BEV) in 2020.[4] While we are aware that most people leave a cornucopia of movement traces due to their use of existing technology (e.g., cell phones), we think that technical solutions for emerging fields, like electric mobility, should be designed with privacy in mind.

Second, at least for the time being, the capacity of most electric vehicle batteries is rather limited, thus most EVs require relatively frequent charging using the growing network of charging stations (CSs) - the European Commission aims at 795,000 public charging stations throughout the EU by the year 2020.[5] The increasing availability of public charging stations is positive and necessary for the success of EVs. However, in combination with the need to charge frequently, it renders vehicle movement profiles more detailed than those derived from fossil fuel not paid with cash.

Third, cash is not an option for almost all utilities. In most parts of the developed world, utilities deliver energy either based on a subscription (post-paid) or pre-paid model where the customer's name is known. In contrast to the current network of fuel stations, EV charging infrastructure is much more distributed, which makes cash logistics prohibitively expensive.

Fourth, the sales of electric energy are tightly regulated in many countries. Many of these regulations aim at making the market more transparent to the customer. However, when applied to the relatively new EV scenario some of these requirements can compromise the locational privacy of the customer.

Contributions. In this paper, we propose a system to authenticate non-anonymous transactions, while preserving users' locational privacy. We use the example of electric vehicle charging, as it offers several interesting constraints. More precisely, we make the following contributions:

- We adapt a carefully chosen group signature scheme without compromising its strong security properties to allow for full compliance with regulations and legal requirements. These requirements were identified with the help of experts in the field of commercial law and energy law. The privacy mechanisms protecting the user's location data are very strong: not only is it impossible to decide whether a user has charged her vehicle at a specific CS, it is even impossible to decide whether a user has *ever* been charging at one or several CSs more than once.
- Our solution is complete, in that it covers the charging process from after authentication to providing all information necessary for the clearing process. It closely fits existing clearing and billing structures and can be implemented efficiently on a large-scale.
- To the best of our knowledge, we are the first to also offer an implementation of a practical charging and billing system for electric vehicles that provides strong protection of the customer's locational privacy. Our implementation performs well even on the limited hardware of a CS, while we are able to process more than one million charging processes per

[4] Pike Research, Electric Vehicle Market Forecasts, http://www.pikeresearch.com/research/electric-vehicle-market-forecasts, 2013, accessed January 29, 2013.

[5] cars21.com, EU proposes minimum of 8 million EV charging points by 2020, http://beta.cars21.com/news/view/5171, 2013, accessed January 29, 2013.

hour using off-the-shelf hardware at the backend (BE), thus providing a cost-effective way to process billing information from a large network of CSs.

2 Overview

The system we propose consists of three main phases: (1) authenticating the customer, (2) authenticating the tuple of customer identity and energy consumption data, and (3) transmitting this data to a clearing house, all without compromising the customer's locational privacy. In the following, we first lay out the problem space before presenting our scheme.

2.1 Problem Space

We define the problem space as follows: Electric utility companies that are honest but curious and want to learn about past, present, and future locations of vehicles, or any entity obtaining (billing) records from utilities, can infer a movement profile for every customer, based on these records. Under the assumption that

a) the creation of movement profiles without explicit consent of the subject is undesirable and the existence of unnecessary data is to be avoided,

b) anonymous payments are not an option,

c) the solution should integrate well with existing billing infrastructure and processes

we explore how the creation of movement profiles can be prevented, while integrity, authenticity, and, in parts, the confidentiality of the data transmitted between a point of sale (i.e., a CS) and a backend is provided. Conceptually, we thus must deviate from the widespread paradigm of anonymizing customers in privacy-enhancing payment and billing systems. Instead, our approach to this problem is to *anonymize locations*, i.e., to cryptographically ensure that charging station locations cannot be linked to customers' identities and timestamps. In this context we identify three core issues:

One way to cryptographically bind a customer identity to metering data are digital signature algorithms, as they achieve non-repudiation. However, the location where a charging process took place can be directly inferred, classical digital signatures not only guarantee the authenticity of the signed data, but also authenticate entities, i.e., the respective charging station (Issue 1). Location-bound tokens, like the identifier of the energy meter used for the measurement, naturally compromise the customer's locations, but utilities are legally required to retain this information in many European countries (Issue 2). The location of a transaction can also be inferred from network-based identifiers (Issue 3), primarily the charging station's IP address, e.g., by correlating BE server access logs with billing data timestamps.

Furthermore, an entity may have access to the network that connects the backend or a CS to the Internet. Such an attacker might try to infer the origin of a message by using a timing side channel, but must be unable to attribute the connection to a specific user.

We assume that all attackers are computationally bound and accordingly unable to break computationally hard cryptographic primitives. Attacks against the point of sales itself are out of scope of this paper.

2.2 Approach

We address *Issue 1* by employing a group signature scheme with strong security properties that provides very efficient verification procedures for large numbers of signatures as a central building block of our system. The scheme allows for the conditional identification of a signer, while in the

default case allowing him to remain anonymous. For every entity that is not in possession of the so-called opening key, the actual signer of a message is indistinguishable from every other potential signer within the same group. Thus, while a customer's transaction is always linked to his customer account, our system guarantees unlinkability with respect to location and time of a transaction.

We address *Issue 2* by modifying the signature scheme such that information that is required by law or regulations, but would compromise the customers' locational privacy, is also only conditionally available. In normal operation this information is as strongly protected, as the signer's identity itself. In case of a legal dispute, where this information must be produced by the utility in front of a court of law, such that an independent entity can assess the proper calibration of the energy meter, the identifier of charging station and energy meter can be revealed by a trusted third party. Legally required information for Germany was identified with the help of our colleagues from the faculty of law, who specialize in commercial law and energy law. However, we present a generalized approach, i.e., the exact datum required in the respective jurisdiction is secondary: if the information is location-bound, it can be afforded the aforementioned strong cryptographic protection. Thus, our approach is adaptable and usable in arbitrary national and international contexts.

We are aware that in being compliant with legal regulation, our system also depends on legal protection: A high legal hurdle must be placed before the identification of a signer (i.e., the respective CS) and the disclosure of location-bound tokens. This could mean, for example, that a court order or the customer's consent is required, not only in case of a dispute between customer and vendor, but especially in the context of criminal law.

We address *Issue 3* by anonymizing the sender of billing-relevant information on the network level. As the communication between charging station and backend is not highly time critical, we could in principle use high-latency mix networks, such as Mixminion[6] or Mixmaster.[7] However, as network availability is an issue, we chose to use the, at the time being, most popular anonymity network, which increasingly offers good redundancy due to its high number of nodes: the Tor network.[8] As Tor does not provide protection against exploiting timing side channels, especially in the presence of low traffic volume, we also discuss how these kinds of attacks can be mitigated in our application context. Please note however that Tor is only one tool in this context and could be replaced by another anonymity network.

In summary, the authentication and charging process we propose is as follows (cf. Figure 1):

1. The CS authenticates towards the customer and vice versa. The CS retains the authenticated customer identity.
2. Upon successful authentication, the CS's power outlet is unlocked and/or put on-line. Charging begins as soon as the EV is connected.
3. When the power-line connection between the CS and the EV is interrupted, the CS generates a tuple containing all information required for the billing process (i.e., the authenticated customer identity stored from Step 1, the amount of energy provided to the user, a timestamp indicating the beginning of the charging process and a timestamp indicating its end). Each location-bound token that is legally required is encrypted to the single entity in possession of the opening key, a trusted third party, denoted as the opener. The tuple is signed using the group secret xi of the respective CS and the data is transmitted to the BE via the Tor network. To ensure confidentiality of the transmitted data, we establish a TLS tunnel

[6] George Danezis, Roger Dingledine, and Nick Mathewson, “Mixminion: Design of a type III anonymous remailer protocol," in *IEEE Symposium on Security and Privacy*, (2003).

[7] Ulf Möller et al., *Mixmaster Protocol* | Version 2, http://www.abditum.com/mixmaster-spec.txt, 2003.

[8] Roger Dingledine, Nick Mathewson, and Paul Syverson, “Tor: the second-generation onion router," in *13th USENIX Security Symposium* (2004).

between CS and BE prior to transmission. Our approach also addresses the relevant use case of customers roaming between energy providers, which we detail in Section 2.3.

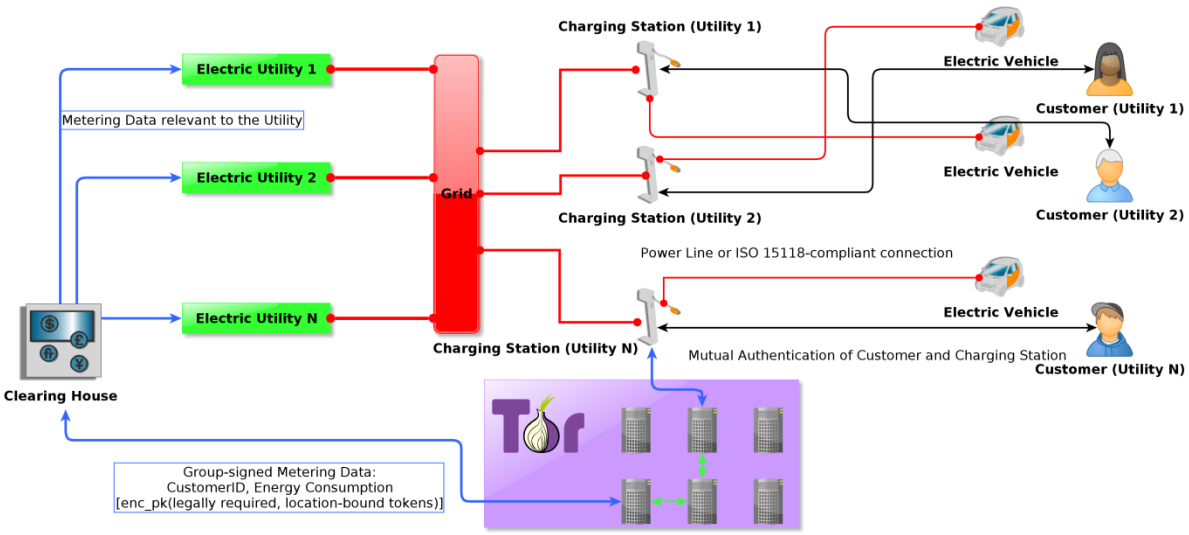

Figure 1: Charging and Transmission of Metering Data (including roaming use case)

2.3 Roaming

While a significant part of customers can still only charge at CSs owned by the utility they have a contract with, roaming is desired by most market participants. In Figure 1 the concept is represented by the introduction of a clearing house. Following the example of the banking and telecommunications sector, at least two parallel efforts[9] are already under way in the energy sector to establish a clearing house to back a roaming-enabled charging infrastructure for electric vehicles. As the clearing house aggregates and verifies metering data from all the CSs, it is capable to provide either only data clearing or also financial clearing to the associated electric utility companies, which in turn allows each utility's customers to roam freely between all other utilities cooperating with the clearing house.

3 System Design

In this section we describe all processes that constitute our system. Group signature schemes are an essential part of our approach and thus we explain below how we utilize and adapt this concept and why we chose the *eXtremely Short Group Signature* (XSGS) scheme.

3.1 Group Signatures and XSGS

The idea of group signature schemes has first been introduced by Chaum and van Heyst in 1991.[10] A group signature scheme is a digital signature scheme that (additionally) provides a (strong) form of sender-anonymity. Unlike in classical signature schemes where each signature is produced by a single signer, in a group signature scheme each signature is produced on behalf of a group. For the verifier it is easy to check whether the signature has been produced by one of the current *group members*. However, finding out who exactly produced the group signature is impossible. Intuitively, the larger

[9] https://www.e-clearing.net/; http://www.hubject.com
[10] David Chaum and Eugène van Heyst, “Group Signatures" in *EUROCRYPT* (1991), 257-265.

the group is, the better are the anonymity guarantees provided for each group member - an ideal property for our scenario.

Anonymity: Pseudonyms vs. Group Signatures. Group signatures provide a very strong form of anonymity that is usually referred to as unlinkability: it is not only impossible to map a signature to its creator - this could be achieved by pseudonyms alone. Unlinkability also implies that no one, except for a dedicated trusted party called opener, is able to decide whether two group signatures have been produced by the same signer. We believe that for our application this property is crucial.[11] When using pseudonyms for CSs alone to protect the user's locational privacy, the verifier could easily build up customer profiles for every CS which, with more and more user-dependent billing data, could possibly be narrowed down to a single CS. In this way one could easily reveal the true CSs behind the pseudonyms. As a consequence, the verifier could easily follow where and when each user charged its vehicle. Group signatures on the other hand do not even reveal whether two signatures belong to the same CS. So users who constantly charge their vehicle at the same CS are indistinguishable from those who travel a lot and often use CSs that they have never visited before.

Design Features of the XSGS Scheme. Group signatures vary in the extent of functionality they offer and in the security guarantees they provide for group members and verifiers. In our work, we utilize the *XSGS scheme* by Delerable and Pointcheval.[12] The XSGS scheme is an extended variant of the well-known group signature scheme by Boneh, Boyen and Shacham (BBS) which achieves very high efficiency with respect to both signature size and speed.[13] It modifies the BBS scheme in two ways. First, it adds improved protection of group members against collusions of (corrupted) members who try to frame a user. In XSGS, even if the issuer itself is corrupted and takes part in that collusion, its honest group members cannot be framed. Second, XSGS guarantees unlinkability of signatures to even hold against an adversary that can convince the opener to open all other signatures. BBS does in general not cover such attacks (not even when the adversary may convince the opener only once). As a theoretical benefit of these extensions, the XSGS scheme can be proven secure in the very strong security model of Bellare, Shi, and Zhang.[14] We believe that these extended properties of XSGS are necessary in our application. In particular, they allow to implement the issuer at the same place as the (only) verifier (i.e., the clearing house), without risking the CS's anonymity. In the selected context this property implies that the clearing house may act as group manager *and* initial verifier, removing administrative and computational work load from the participating energy providers, without compromising the systems' security guarantees.

Support for Batch Verification. An important design restriction of our solution is that we consider a single verifier that has to verify a huge amount of signatures. The group members, on the other hand, do only have to generate a moderate amount of signatures each day. Thus our group signature scheme should ideally feature very fast verification procedures. Kim et al. showed that XSGS supports batch verification.[15] For security reasons, the combination process is setup in such a way that adversaries cannot produce a combination of invalid signatures which pass the batch verification test.[16]

[11] We recall once again that user identities have to be known to the verifier for a proper billing process. Thus it is not possible to anonymize user identities in the bills.

[12] Cécile Delerable and David Pointcheval, "Dynamic Fully Anonymous Short Group Signatures" in *VIETCRYPT* (2006), 193-210.

[13] Dan Boneh, Xavier Boyen, and Hovav Shacham, "Short Group Signatures" in *CRYPTO* (2004), 41-55.

[14] Mihir Bellare, Haixia Shi, and Chong Zhang, "Foundations of Group Signatures: The Case of Dynamic Groups" in *CT-RSA* (2005), 136-153.

[15] Kitae Kim et al., "Batch Verification and Finding Invalid Signatures in a Group Signature Scheme," I. J. *Network Security* 13, no. 2 (2011): 61-70.

[16] The batch verifier of Kim et al. uses the so-called small exponent test. Mihir Bellare, Juan A. Garay, and Tal Rabin, "Fast Batch Verification for Modular Exponentiation and Digital Signatures" in *EUROCRYPT* (1998), 236-250.

Dynamic Groups. XSGS allows for dynamic groups, i.e., group members can be added and removed without re-initializing the whole scheme. Also, member joins do not require updates of the group public key GPK. We stress that if member joins do not require modifications of GPK, it is necessary to modify the group public key when revoking users. In the setting at hand, where the system is likely to expand, not needing to recalculate the GPK for every new CS improves overall system performance. Instead, the system-wide update of GPK is only required when a CS is removed. However, even then the approach for updating the GPK underlying XSGS is very efficient. It is based on dynamic accumulators.[17]

3.2 Bootstrapping the System

Before we can start authenticating users, charging vehicles, and securely transmitting energy consumption data, we have to set up the infrastructure. The clearing house acts as the group manager within the XSGS scheme. It can add a new CS to the group by issuing a user certificate (credential) $UCert$ to CS. A CS with a valid $UCert$ is also referred to as a group member. The clearing house can also revoke the ability of group members to sign on behalf of the group. An entity sufficiently independent of the clearing house serves as the opener. In our scenario N electric utilities choose to cooperate by utilizing a certain clearing house. Each utility i provides m_i charging stations to the public.

In order to bootstrap the XSGS scheme, the group manager first needs to generate the group (curve) parameters of a bilinear group (including group descriptions, generators, and pairing specification). Technically, the bilinear group consists of two elliptic curve groups $\boldsymbol{G_1}$ and $\boldsymbol{G_2}$ of prime order p with random generators $G_1 \in \boldsymbol{G_1}$ and $H, G_2 \in \boldsymbol{G_2}$ and the description of a non-degenerated bilinear pairing e: $G_1 \times G_2 \rightarrow G_t$ such that $e(G_1^a; G_2^b) = e(G_1; G_2)^{ab}$ for every $a, b \in \boldsymbol{Z_p}$. For more details we refer to Boneh, Boyen and Shaham[18]. Next it generates a secret Diffie-Hellman key $IK \in \boldsymbol{Z_p}$ (called issuer key) with its corresponding public key $= G_2^{IK}$.

The issuer key IK is used to generate certificates for new group members. Given these values, the opener generates a private key of a chosen-ciphertext secure encryption system, the opening key OK. The corresponding public encryption key is denoted as OPK. The public key OPK is used in the signing process of the group signature scheme to encrypt the signer's certificate $UCert$. This enables the opener to reveal which CS has actually created a given group signature. On a technical level OK consist of two independent secret keys of an ElGamal encryption system. OPK contains the corresponding public keys. It is well known that ElGamal is only chosen-plaintext secure. However, the system applies the well-known Naor-Yung transformation[19] which encrypts a given messsage under both ElGamal keys resulting in ciphertext $Z_1$and Z_2. Additionally, it generates a NIZK proof P of equality of plaintexts in $Z_1$and Z_2. The ciphertext Z consist of $Z = (Z_1; Z_2; P)$. The group public key GPK consist of the paramaters of the bilinear group, W, and OPK. Besides these values we also require that a public RSA modulus n is available to all parties. This value is generated by a trusted third party. The corresponding secret key is deleted. The setup procedure is depicted in Figure 2.

[17] Jan Camenisch and Anna Lysyanskaya, “Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials" in *CRYPTO* (2002), 61-76; Lan Nguyen, “Accumulators from Bilinear Pairings and Applications," in *CT-RSA* (2005), 275-292.

[18] Boneh, Boyen, and Shacham, “Short Group Signatures." in CRYPTO (2004)

[19] Moni Naor and Moti Yung, “Universal One-Way Hash Functions and their Cryptographic Applications," in *STOC* (1989)

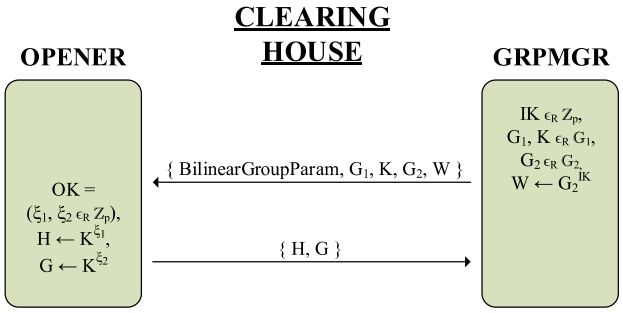

Figure 2: Setup Phase

3.3 Setting Up New Charging Stations

Each new CS must join the group before it can sign metering data. Now that group manager and opener are set up, the group manager can add new charging stations to the group. Note that all charging stations, independent of the utility that operates them, will be members of the same group.

The group manager starts the join process by transmitting the GPK to the CS. The CS draws its private signing key $UK \in \boldsymbol{Z_p}$ and computes a commitment $C = H^{UK}$ of UK. Then it sends C together with a NIZK proof of knowledge of UK to the group manager. On successful verification of this proof, the group manager selects a random signing key $x \in \boldsymbol{Z_p}$ for the CS and calculates the group member identifier

$$A = (G_1 \cdot C)^{\frac{1}{IK+x}} \Leftrightarrow e(A, W \cdot G_2^x) = e(G_1 \cdot C, G_2)$$

The values A and x constitute the certificate $UCert$ of the CS. Intuitively, $UCert$ is a digital signature over x that can only be computed with the help of *IK*. The group manager first sends A to the CS and proves that it knows a corresponding x that fulfills the above equation.
Knowing that its communication partner can indeed issue certificates, the CS produces a classical signature S using its USK over A as $S = Sign_{USK}(A)$ and sends $(S, cert_{CS})$ to the issuer. This pair is important when resolving disputes as it binds the anonymous certificate $UCert$ to a concrete CS that can be identified via the classical PKI. If the signature is valid, the group manager sends x to the CS and registers the entry $(UCert, C, cert_{CS}, S)$ in a database. Now since $C = H^{UK}$ and UK is known to the CS we get that

$$A = (G_1 \cdot H^{UK})^{\frac{1}{IK+x}} \Leftrightarrow e(A, W \cdot G_2^x) = e(G_1 \cdot H^{UK}, G_2)$$

The join process is depicted in Figure 3.

3.4 Decommission of Charging Stations

Occasionally it may be necessary to remove a CS from the group, be it because it is replaced by a CS of a newer generation or to deal with a compromise. We consider the revocation of a group member's credentials to be a less frequent event than the joining of a new member. Thus, while $UCert$ and UK remain unchanged upon the joining of a new member, removing a member from the group requires that all remaining group members receive information on how to re-calculate their group identifiers A.

Assume the group manager wants to revoke a CS with

$$UCert' = (A', x').$$

First, it publishes an updated version of the GPK. For example $G_1, G_2,$ and H are substituted by

$G_1^* = G_1^{\frac{1}{IK+x'}}, G_2^* = G_2^{\frac{1}{IK+x'}}$, and $H^* = H^{\frac{1}{IK+x'}}$. each group member with $UCert = (A, x)$ and secret key UK except for the one to be revoked has to update its group identifier

$$A^* = A^{\frac{1}{IK+x'}}$$

To this end it is sufficient that the group manager simply publishes x'.

$$A^* = A^{\frac{1}{IK+x'}} = \left(G_1^* \cdot H^{*UK} \cdot A^{-1}\right)^{\frac{1}{(x-x')}}.$$

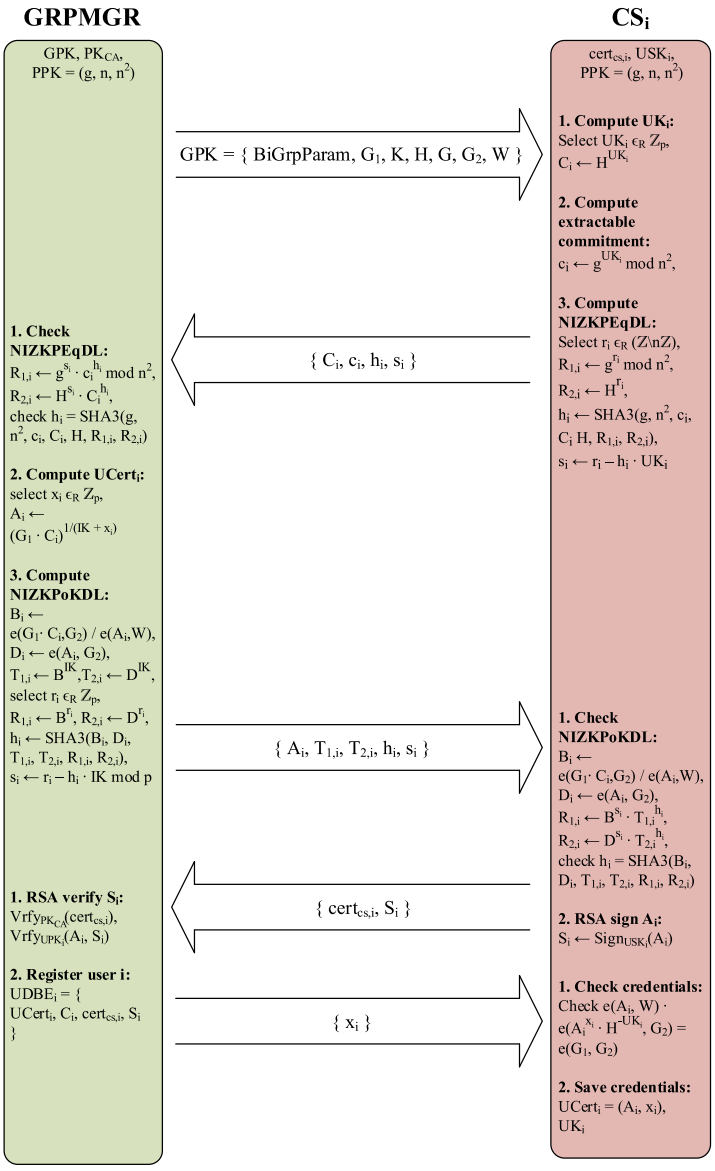

Figure 3: Join Procedure

Next, each charging station computes a new signature $S = Sign_{USK}(A^*)$ over the new group member identifier A^* and sends it to the group manager. The group manager verifies S^* from each CS and, on success, updates the existing database entries with the new values for A^*, C^* and S^*. Note that the CSs do not have to save an incremental revocation list of all revoked members to decide on the validity of newly signed metering data. However, it might be necessary for the group manager to retain a limited set of old group credentials for the time span that the respective jurisdiction sets for

the resolution of disputes concerning past charging processes. The revocation process is depicted in Figure 4.

3.5 Ensuring Authenticity of Metering Data

When the charging process is terminated (i.e., the cable connection between EV and CS is severed), the CS creates a message M consisting of the authenticated customer identity, the amount of energy consumed by the customer, two timestamps marking the beginning and the end of the charging process, and a string that identifies the utility owning the CS. As discussed above, legal regulations often requires transmission and storage of the identifier (*meterID*) of the calibrated energy meter or of other certified components of a point of sale.

These identifiers would reveal the physical location of the transaction. To avoid this, we have to adapt the group signature scheme slightly. Instead of being sent in the clear, the *meterID* is encrypted using the opener's encryption key OPK before being added to M. In the same way other location-critical information can be incorporated into the group signature. Only the opener can decrypt these values using its secret decryption key OSK. We stress that while the *meterID* is always encrypted with the opener's public key and never transmitted in the clear, it is not necessary to prove that the correct *meterID* has been incorporated into the ciphertext. The opener can uniquely identify the CS and any incorrect information of a CS on its *meterID* can thus easily be revealed. As sketched above, CS's group signature s on M consists of an encryption Z of $UCert$ and a message-dependent NIZK proof showing that CS knows a valid $UCert$ with corresponding UK which fulfill Equation 2 and that $UCert$ has been encrypted correctly under public key OPK in the ciphertext Z (which is part of s).

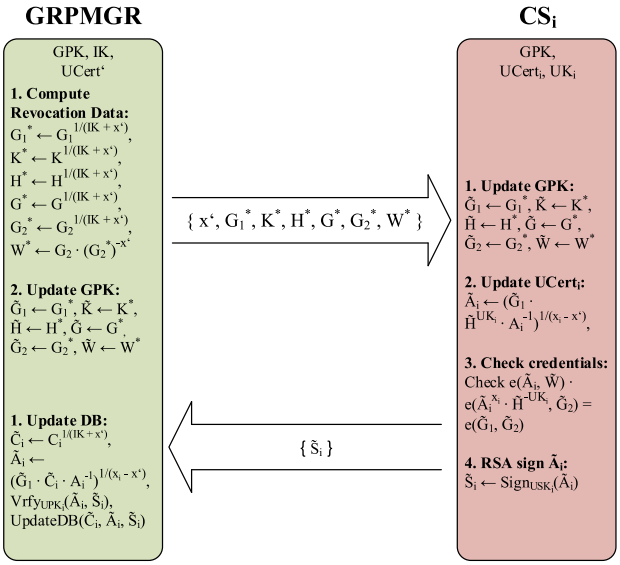

Figure 4: Revocation Procedure

Intuitively, these types of message-dependent proofs work like signatures. Generating them on a messages M requires the creator to know A, x, and UK. They are often referred to as signatures of

knowledge.[20] The entire signing process is depicted in Figure 5. For more details on the computations of the group signature, we refer to the literature.[21]

3.6 Transmission of Metering Data

To prevent the disclosure of the CS's network location, the CS first connects to the Tor network and establishes a routing circuit. It then starts a TLS session with the backend (BE) and in the process verifies the certificate presented by BE. We use a ciphersuite based on Ephemeral Diffie-Hellman (DHE) with CBC-MAC, as it offers perfect forward secrecy and because of its cryptographic security properties: it has recently be shown to be provably secure in a strong security model.[22] We rely on TLS to guarantee that each transmission from a CS reaches the backend. Although Tor provides sender anonymity, a possible timing side channel exists: if there is only sporadic network traffic within the system of CSs and BE, an attacker observing both the network at a CS and the BE could correlate these events with charging timestamps (somehow obtained) from the clearing house. As the transmission of billing relevant data is not time-critical in the example of EV charging, we can prevent correlation as follows:

each CS is scheduled to send a transmission of a given size once per 15 minutes. Each charging process results in one message of typically less than 1000 Byte. If we fix the size of the transmission, for instance, at 5 kByte, it fits several messages (M, s). We pad each transmission with random data to the maximum size. If a message (M, s) does not fit in the current transmission anymore, it is scheduled for the next. If no charging process has been finished within the time window, we just transmit the string empty and pad the transmission to the defined maximum size. As all transmissions are of equal size and are encrypted as described above, an attacker observing the network is unable to distinguish between transmissions that contain billing data and those that do not. The BE acknowledges the successful submission by sending the string ACK and a timestamp. We rely on TLS for the authenticity of the reply.

3.7 Verification of Metering Data

When the BE at the clearing house has received *(M,s)* it verifies the group signature s by checking the NIZK proof with respect to the GPK and thus determines whether the consumption data that is bound to the identity of a customer is valid. For details on the computations, we refer to.[23] If the signature does not verify it simply discards the message as it cannot stem from a CS within the group. On success, the signed tuple M is passed on to the clearing service for processing. As there is one central verifier in the system that verifies all metering data, batch verification of group signatures offers a significant efficiency gain.

3.8 Dispute Resolution

In the case of a dispute, the opener can craft a non-repudiable publicly verifiable proof of the actual creator of a given group signature. The opener will act so only upon the request of a judge or with the consent of the customer. Note that even after a message M_i has been subject to the opening process, it is impossible to decide, whether a CS who signed M_i also signed a different message M_j, i.e, the location of other, potentially unrelated charging events remains hidden. To open the

[20] Melissa Chase and Anna Lysyanskaya, „On Signatures of Knowledge," in *CRYPTO* (2006), 78-96.

[21] Kim et al., „Batch Verification and Finding Invalid Signatures in a Group Signature Scheme"; Delerable and Pointcheval, „Dynamic Fully Anonymous Short Group Signatures."

[22] Tibor Jager et al., „On the Security of TLS-DHE in the Standard Model" in *Advances in Cryptology - CRYPTO* (2012).

[23] Kim et al., „Batch Verification and Finding Invalid Signatures in a Group Signature Scheme";Delerable and Pointcheval, „Dynamic Fully Anonymous Short Group Signatures".

signature s, the opener uses its secret opening key OK to decrypt the ciphertext Z and obtain the certificate $UCert$ of the signer. Next it uses its access to the registration database to obtain UPK and S which correspond to $UCert$. From this information she computes a publicly verifiable NIZK proof that $UCert$ is actually encrypted in Z. Together with the database entry $A, certCS, S$ this convincingly reveals the identity of the signer in a non-reputable way.

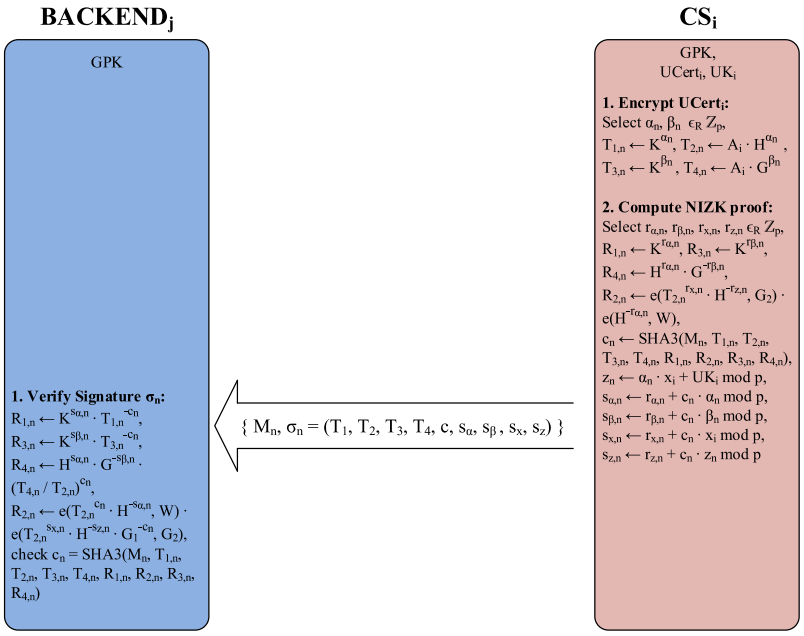

Figure 5: Sign Procedure

4 Evaluation

In this section, we describe how we evaluated our prototype implementation. We also present an overview of the performance results obtained both for the various operations of the XSGS scheme and the transmission of data from a CS to the BE. For implementation details, please refer to Appendix A; for the choice of cryptographic parameters, please refer to Appendix B.

4.1 Evaluation Environment

We aimed at evaluating our approach in a realistic environment. Thus, we implemented XSGS and tested the creation of signed messages, the setup process for adding new charging stations, and the procedure to decommission charging stations on a prototype of a CS for EVs built at our department. The CS contains an inexpensive industrial-grade Intel Atom platform (CS_1, cf. Table 1) as control unit that interacts with the energy flow control subsystems within the CS and acts as a front-end to the user. Additionally, we evaluated our implementation on a Freescale i.MX53, which is an implementation of an ARM A8 core. Comparable platforms to both variants can be found in CSs in the market or under development today.

As BE we chose an Intel server platform (cf. Table 1). We used this platform to evaluate all XSGS operations typically performed by the group manager, opener, judge, or any entity that wishes to verify a signature. We also created signatures and performed join operations as a comparison to the measurements on the actual CS. While the Tor network is widely used and considered usable for

non-time critical applications, we also used this platform to evaluate if latency and throughput are acceptable in our application scenario.

Table 1: Evaluation Environment

	Hardware Platform	OS
CS_1	Intel Atom D2550, 1GB RAM	Ubuntu 12.04
CS_2	Freescale i.MX53, 1GB RAM	Ubuntu 10.04
BE	Intel Xeon X5650, 2GB RAM	Ubuntu 12.04

4.2 Evaluation Results

We performed the setup procedure required for adding a new CS 100 times. The computations necessary on the CS are performed on average in 757.4 ms on CS_1 and 1077.3 ms on CS_2, while the computations on the BE took 55 ms on average. Accordingly, we performed 100 decommission procedures: on average, the computations performed on CS_1 take 49.0 ms (resp. 77.8 ms on CS_2), the computations on the BE take 20 ms. We also performed 100 dispute resolution procedures on the BE: on average opening a message takes 8.2 ms, while judging takes 6.9 ms.

We evaluate the time required to prepare a message to transmit the metering data to the BE. Preparing a message 1000 bytes (taken from /dev/urandom) takes 28.5 ms on average on CS_1; on CS_2 the process takes 41.5 ms. Preparing a message that allows for batch verification on the BE takes slightly longer: 28.8 ms on CS_1 or 43.1 ms on CS_2. For a message size up to 100,000 bytes message creation takes less than 33 ms on CS_1 and 54.2 ms on CS_2. Figure 2 shows that the size of the message only has a limited impact on the time required to create a valid signature, as we only sign a hash of the message. Creating a signed message of one million bytes takes 66.7 ms on average on CS_1 and 161.1 ms on CS_2. These results show that ensuring the authenticity of messages by means of group signatures is feasible on the limited hardware found in a CS. Even more so, as we only need to generate one signature for each charging process.

Being able to batch verify messages offers a significant performance increase. While a CS will typically only create one message every few minutes or every few hours, each message has to be verified by the BE. The verification of a normal message takes 30 ms, a single batch-enabled one is verified in about the same time. Figure 3 shows that verification time increases linearly with the amount of messages. Standard verification allows for processing 41 messages per second on the BE, while batch verification allows for processing of 93 messages in the same time. When comparing the time required for verifying one thousand messages, batch verification is about 2.3 times faster. In a worst case scenario, where a batch contains so many invalid signatures that it is faster to verify each individual message, we can still process 147,600 messages per hour using a single CPU core. As the process can be parallelized at will, a comparable server with eight CPUs cores instead of one is sufficient for processing more than one million messages per hour.

As transmission times vary due to network latency, we evaluate the network performance separately: We used iperf[24] to measure whether the Tor network offers enough bandwidth for transmitting metering data from the CS to the BE. We controlled that the bandwidth between the host running the iperf server and and the one running the client is not the limiting factor and repeated our measurements at various times of the day, building a new Tor circuit for each iteration. We were able to transfer a minimum of 373 kbit per second and a maximum of 1.07 Mbits per second through the Tor network. While the actual throughput may vary depending on the time of day and the chosen circuit, our evaluation shows that it is reasonable to assume that we can transfer

[24] http://iperf.sourceforge.net/

metering data through the Tor network, especially as the communication between CS and BE is not subject to real-time requirements. Also note that the BE is not affected by Tor's limited bandwidth, as there is no need to obscure the BE's location and only CSs communicate via Tor. We expect that anyone willing to operate a large-scale commercial system, that relies on a anonymity network like Tor, will need to contribute to the infrastructure of the respective anonymity network to increase dependability and throughput. Thus, as a positive side-effect, a large-scale application of the respective anonymity network would strengthen the overall availability and resources of this anonymity network.

In summary, we found that our approach performed well on all tested platforms and, most importantly, is fast enough for our application.

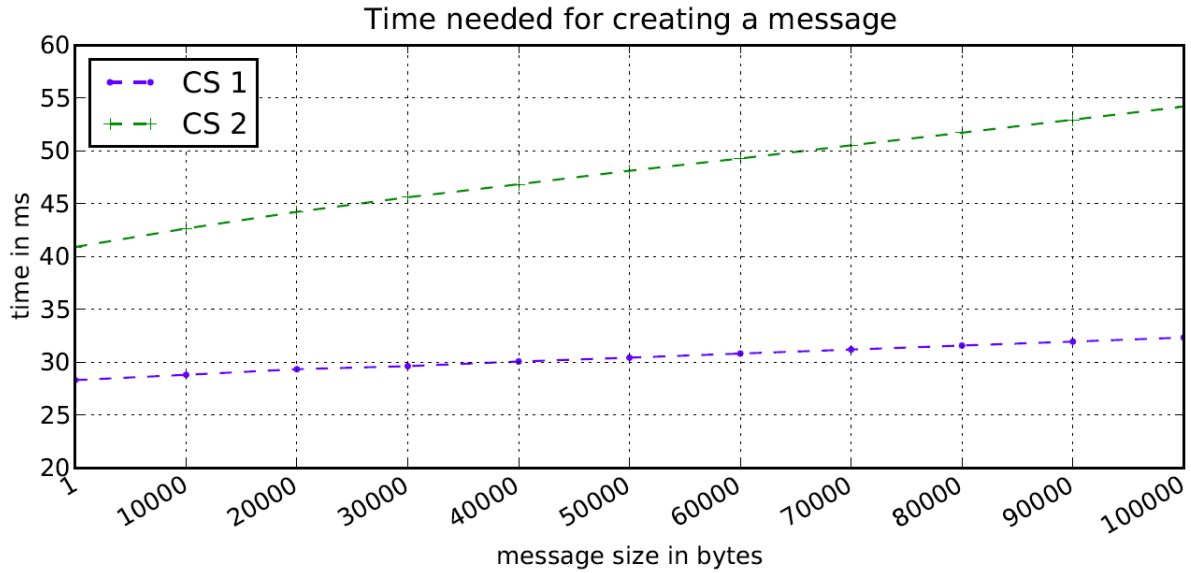

Figure 6: Time required for message creation by size

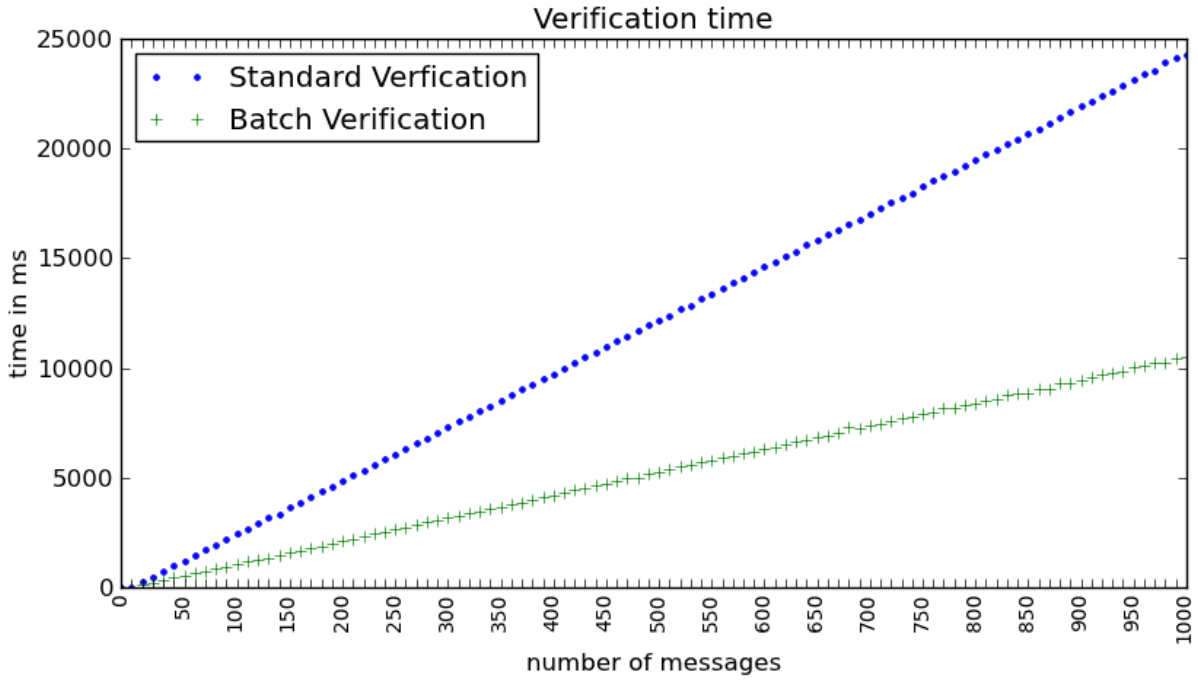

Figure 7: Time required for verification by #messages received

5 Discussion

We now discuss possible attacks against both the authenticity of billing-relevant data and against the user's locational privacy.

5.1 Malicious Customer

While our system is well equipped to counter attackers with capabilities as described in Section 2.1, there exists the theoretical possibility that an attacker, who is a valid customer in the system, could force a CS_1 offline before a revocation of a different CS_2 takes place. Thus, CS_1 does not realize that the group credentials have changed and must be recomputed. The attacker then authenticates herself and charges her EV at CS_1, which is possible as user authentication works offline. The CS signs the metering data with its current credentials. At some point in the future, when the CS is online again, it transmits the data to the BE. It will then also receive new group credentials and will be able to create valid messages, as during the revocation process. Still, the BE will discard the delayed metering data from the CS as it has been generated with the old credentials. Hence, the attacker was able to charge for free in the meantime. There are at least two counters to this attack. First, if the CS is up and running again, it may simply re-sign all the unsent metering data with the updated credential. Second, if the CS is for some reason not able to continue signature generation (for example if a trusted key storage is broken), we can still retain old credentials for verification and use the old group signature to bill the customer correctly.

5.2 Tracking and Localization Attacks

Ma et al. show that if a set of traces of time and corresponding location of mobiles nodes exist, where '[t]he traces are anonymous in that the true identity of a participant has been replaced by a random and unique identifier'[25], a small amount of side information is sufficient for an attacker to infer the true identity of a user. The work of de Montjoye et al.[26] supports these claims and shows that even datasets with coarse traces provide little anonymity, in such that four spatio-temporal points are enough to uniquely identify 95% of the individuals.

However, neither approach is applicable to our system. Due to the nature our approach, no spatio-temporal data points, let alone location tracks, are available to any entity except the opener. Thus Krumm's inference attacks[27], which aim at de-anonymizing entities from anonymous or pseudonymous location tracks, are not applicable in the setting at hand. We do not conceal the identity of the user, but cryptographically protect their location. To thwart attacks by third parties (i.e., non-legitimate receivers of transmitted data), all information is transmitted encrypted with a provably secure TLS variant. Thus the attacker needs to be a legitimate receiver of the data, i.e., the clearing house or a utility. Both receive the following information: customer A of utility B consumed N kWh of energy, starting from timestamp X, ending at timestamp Y. Every location-bound token, like the CS's public key and the *meterID*, is encrypted only to the opener and thus never leaked to any other party. Thus, the only entity able to access location data at will is the opener, who is explicitly trusted. Given the exposed position of the opener as a trusted third party, it is mandatory for this party to be independent from all other parties (i.e., from vendors, customers, intermediaries, law enforcement etc.) in a commercial deployment of the system. However, the concrete instantiation of this trusted third party is both an organizational and a political question, which is beyond the scope of this technical paper.

[25] Chris Y.T. Ma et al., „Privacy vulnerability of published anonymous mobility traces," in *MobiCom '10* (2010).
[26] Yves-Alexandre de Montjoye et al., „Unique in the Crowd: The privacy bounds of human mobility", *Scientific Reports*, 2013, http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html.
[27] John Krumm, „Inference Attacks on Location Tracks", in Pervasive Computing (Pervasive 2007)

As we necessarily need to exclude any trusted third party from the group of potential attackers, the data available to an adversary thus does not contain the location of the user, nor can the attacker use the amount of energy consumed to infer the distance the user has driven between two charging events, due to external factors that influence power consumption, like driving style, speed, etc. Shokri et al.[28] propose a metric to quantify the performance of a location privacy protection mechanism (LPPM). Our systems applies location hiding as an online LPPM in a distributed architecture, i.e., we only look at the current event at the time of its creation and hide all location-bound information by encrypting it to the opener. As argued above, while records of user interaction exists for billing purposes, they do not contain any spatio-temporal locations or references to such data. An adversary, who knows the location of every CS, may determine the location where the EV could have been charged with a high accuracy (as it was necessarily at the location of a CS), but he is unable to achieve a high correctness as to where the EV was actually charged.

6 Related Work

Locational privacy has been recognized as being desirable as early as 1996.[29] Its importance has been recognized for example in the field of pervasive computing[30] and also in the context of location-based mobile applications.[31] The importance of location privacy in the context of transportation is underlined by numerous publications that aim at preserving location privacy in various applications like vehicular communication systems,[32] ticketing for public transport systems[33], and electronic road toll collection. In the latter context, Balasch et al.[34] use commitments that do not reveal information on the user's location, while relying on a disjoint audit system based on spot checking cameras. In the audit system, user locations are sporadically but routinely linked to identity information. Meiklejohn et al.[35] follow closely the PrETB construction by Balasch et al., but also include malicious colluding users into their threat model. Our approach, in contrast, does not require the routinuous linking of users' locations and identities. We reserve this extreme measure to singular occurances, where a vendor can argue an initial suspicion of misuse. Chen et al.[36] propose the use of a group signature scheme to enhance the users' privacy, by hiding a user's identity within a group while ensuring data integrity and authenticity. Popa et al. [37] anonymize vehicles on the move by using random identifiers (tags) to prevent a server from linking user locations, effectively hiding their identity. However, the authors did not implement the proposed solution and fail to evaluate the feasibility of their approach in the given scenario. A limited amount of publications have considered

[28] Reza Shokri et al., "Quantifying Location Privacy," in *2011 IEEE Symposium on Security and Privacy (SP)* (May 2011), doi:10.1109/SP.2011.18.

[29] Ian Jackson, „Anonymous addresses and confidentiality of location", in *Information Hiding* (1996).

[30] Alastair R. Beresford and Frank Stajano, „Location privacy in pervasive computing", *IEEE Pervasive Computing 2*, no. 1 (March 2003): 46-55, issn: 1536-1268, doi:10.1109/MPRV.2003.1186725.

[31] Raluca Ada Popa et al., „Privacy and accountability for location-based aggregate statistics", in *ACM CCS* (2011).

[32] Jean-Pierre Hubaux, Srdjan Capkun, and Jun Luo, „The security and privacy of smart vehicles," *Security & Privacy, IEEE 2*, no. 3 (2004): 49-55; Florian Dötzer, „Privacy Issues in Vehicular Ad Hoc Networks," in *Privacy Enhancing Technologies* (2006); Julien Freudiger et al., „Mix-zones for location privacy in vehicular networks," in *Win-ITS* (2007); K. Sampigethaya et al., „AMOEBA: Robust Location Privacy Scheme for VANET," *IEEE Journal on Selected Areas in Communications 25*, no. 8 (October 2007): 1569-1589, issn: 0733-8716, doi:10.1109/JSAC.2007.071007; Zhendong Ma, *Location Privacy in Vehicular Communication Systems: a Measurement Approach* (PhD thesis, University of Ulm, 2011).

[33] Thomas S. Heydt-Benjamin et al., „Privacy for Public Transportation", in *Privacy Enhancing Technologies* (2006); Erik-Oliver Blass et al., „PSP: private and secure payment with RFID," in *WPES* (2009); Foteini Baldimtsi et al., „Pay as you go," in *HotPETs* (2012).

[34] Josep Balasch et al., „PrETP: Privacy-Preserving Electronic Toll Pricing," in 19th USENIX Security Symposium (2010).

[35] Sarah Meiklejohn et al., „The Phantom Tollbooth: Privacy-Preserving Electronic Toll Collection in the Presence of Driver Collusion," in *20th USENIX Security Symposium* (2011).

[36] Xihui Chen et al., „A Group Signature Based Electronic Toll Pricing System," in *ARES* (2012).

[37] Raluca Ada Popa, Hari Balakrishnan, and Andrew Blumberg, „VPriv: protecting privacy in location-based vehicular services," in USENIX Security Symposium (2009).

locational privacy in the context of e-mobility so far: Chao Li[38] implement a merchant entity of the Compact e-Cash scheme[39] aimed at a charging station. Liu et al.[40] propose an anonymous electronic payment scheme that supports two-way anonymous payments. Stegelmann's and Kesdogan's approach[41] aims at providing locational privacy in the presence of a smart grid that actively manages EVs as energy buffers. We are not aware of an implementation that allows to evaluate the practicality. While their design incorporates optional anonymity revocation, it relies on an anonymous electronic cash scheme for billing. None of these approaches can be used when anonymous electronic payments are not tolerated by legislation or even just undesired by the vendor.

7 Conclusion

In this paper, we introduced a system that enables locational privacy for financial transactions in the absence of anonymous payments. We focused on the example of re-charging electric vehicles and are able to protect the customer's locational privacy during the whole charging process. Our system also fully supports all requirements needed to bill the customer after the charging process and enables users to roam between different CSs provided by different electric utilities. As such, it covers all relevant aspects required for the charging of EVs. The basic idea of our approach is to adapt a group key signature scheme to the tightly regulated setting of selling electric energy as means of propulsion. We described all protocol steps and outlined how the system can be deployed in practice. In an empirical evaluation, we also demonstrated that the solution has a low overhead and can scale to millions of charging processes per hour (even on off-the-shelf hardware).

References

Balasch, Josep, Alfredo Rial, Carmela Troncoso, Christophe Geuens, Bart Preneel, and Ingrid Verbauwhede. „PrETP: Privacy-Preserving Electronic Toll Pricing." *In 19th USENIX Security Symposium*. 2010.

Baldimtsi, Foteini, Gesine Hinterwalder, Andy Rupp, Anna Lysyanskaya, Christof Paar, and Wayne Burleson. „Pay as you go." In *HotPETs*. 2012.

Bellare, Mihir, Juan A. Garay, and Tal Rabin. „Fast Batch Verification for Modular Exponentiation and Digital Signatures." In *EUROCRYPT*, 236-250. 1998.

Bellare, Mihir, Haixia Shi, and Chong Zhang. „Foundations of Group Signatures: The Case of Dynamic Groups." In *CT-RSA*, 136-153. 2005.

Beresford, Alastair R., and Frank Stajano. „Location privacy in pervasive computing." *IEEE Pervasive Computing 2, no. 1* (March 2003): 46-55. issn: 1536-1268. doi:10.1109/MPRV.2003. 1186725.

Blass, Erik-Oliver, Anil Kurmus, Refik Molva, and Thorsten Strufe. „PSP: private and secure payment with RFID." In *WPES*. 2009.

Blumberg, Andrew J., and Peter Eckersley. On Locational Privacy, and How to Avoid Losing it Forever. Technical report. *Electronic Frontier Foundation*, 2009. Accessed February 4, 2013. https://www.eff.org/wp/locational-privacy.

Boneh, Dan, Xavier Boyen, and Hovav Shacham. „Short Group Signatures." In *CRYPTO*, 41-55. 2004.

[38] Chao Li, *Anonymous Payment Mechanisms for Electric Car Infrastructure*, (master's thesis, LU Leuven, 2011).

[39] Jan Camenisch, Susan Hohenberger, and Anna Lysyanskaya, „Compact E-Cash," in *Advances in Cryptology - EUROCRYPT* (2005).

[40] Joseph Liu et al., „Enhancing Location Privacy for Electric Vehicles (at the right time)," in *ESORICS* (2012).

[41] Mark Stegelmann and Dogan Kesdogan, „Design and Evaluation of a Privacy-Preserving Architecture for Vehicle-to-Grid Interaction," in *EuroPKI* (2012).

Brands, Stefan. „Electronic cash systems based on the representation problem in groups of prime order." In CRYPTO. 1993.

Camenisch, Jan L., Jean-Marc Piveteau, and Markus A. Stadler. „An efficient electronic payment system protecting privacy." In *ESORICS*. 1994.

Camenisch, Jan, Susan Hohenberger, and Anna Lysyanskaya. „Compact E-Cash." In *Advances in Cryptology - EUROCRYPT*. 2005.

Camenisch, Jan, and Anna Lysyanskaya. „Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials." In *CRYPTO*, 61-76. 2002.

cars21.com. EU proposes minimum of 8 million EV charging points by 2020. http://beta.cars21.com/news/view/5171, 2013. Accessed January 29, 2013.

Chao Li. „Anonymous Payment Mechanisms for Electric Car Infrastructure." *Master's thesis*, LU Leuven, 2011.

Chase, Melissa, and Anna Lysyanskaya. „On Signatures of Knowledge." In *CRYPTO*, 78-96. 2006.

Chaum, David. „Blind Signatures for Untraceable Payments." In Advances in Cryptology: Proceedings of *CRYPTO* '82. 1982. „Security without identification: transaction systems to make big brother obsolete." Commun. ACM 28, no. 10 (October 1985): 1030-1044. issn: 0001-0782, accessed January 23, 2013. doi:10.1145/4372.4373. http://doi.acm.org/10.1145/4372.4373.

Chaum, David, Amos Fiat, and Moni Naor. „Untraceable Electronic Cash." *In Advances in Cryptology - CRYPTO*. 1988.

Chaum, David, and Eugne van Heyst. „Group Signatures." In *EUROCRYPT*, 257-265. 1991.

Chen, Xihui, Gabriele Lenzini, Sjouke Mauw, and Jun Pang. „A Group Signature Based Electronic Toll Pricing System." In *ARES*. 2012.

Danezis, George, Roger Dingledine, and Nick Mathewson. „Mixminion: Design of a type III anonymous remailer protocol." In *IEEE Symposium on Security and Privacy*. 2003.

Delerable, Ccile, and David Pointcheval. „Dynamic Fully Anonymous Short Group Signatures." In *VIETCRYPT*, 193-210. 2006.

Dingledine, Roger, Nick Mathewson, and Paul Syverson. „Tor: the second-generation onion router." In *13th USENIX Security Symposium*. 2004.

Dötzer, Florian. „Privacy Issues in Vehicular Ad Hoc Networks." In *Privacy Enhancing Technologies*. 2006.

Freudiger, Julien, Maxim Raya, Mrk Flegyhzi, Panos Papadimitratos, et al. „Mix-zones for location privacy in vehicular networks." In *Win-ITS*. 2007.

Heydt-Benjamin, Thomas S., Hee-Jin Chae, Benessa Defend, and Kevin Fu. „Privacy for Public Transportation." In *Privacy Enhancing Technologies*. 2006.

Hubaux, Jean-Pierre, Srdjan Capkun, and Jun Luo. „The security and privacy of smart vehicles." *Security & Privacy, IEEE 2, no. 3* (2004): 49-55.

Jackson, Ian. „Anonymous addresses and confidentiality of location." In *Information Hiding*. 1996.

Jager, Tibor, Kohlar, Florian, Schäge Sven, and Jörg Schwenk. „On the Security of TLS-DHE in the Standard Model." In *Advances in Cryptology - CRYPTO*. 2012.

Kim, Kitae, Ikkwon Yie, Seongan Lim, and Daehun Nyang. „Batch Verification and Finding Invalid Signatures in a Group Signature Scheme." *I. J. Network Security 13, no. 2* (2011): 61-70.

John Krumm, „Inference Attacks on Location Tracks", in Pervasive Computing (Pervasive 2007)

Liu, Joseph, Man Au, Willy Susilo, and Jianying Zhou. „Enhancing Location Privacy for Electric Vehicles (at the right time)." In *ESORICS*. 2012.

Ma, Chris Y.T., David K.Y. Yau, Nung Kwan Yip, and Nageswara S.V. Rao. „Privacy vulnerability of published anonymous mobility traces." In *MobiCom '10*. 2010.

Ma, Zhendong. „Location Privacy in Vehicular Communication Systems: a Measurement Approach." *PhD diss.*, University of Ulm, 2011.

Meiklejohn, Sarah, Keaton Mowery, Stephen Checkoway, and Hovav Shacham. „The Phantom Tollbooth: Privacy-Preserving Electronic Toll Collection in the Presence of Driver Collusion." In *20th USENIX Security Symposium*. 2011.

Möller, Ulf, Lance Cottrell, Peter Palfrader, and Len Sassaman. Mixmaster Protocol | Version 2. http://www.abditum.com/mixmaster-spec.txt, 2003.

Montjoye, Yves-Alexandre de, Csar A. Hidalgo, Michel Verleysen, and Vincent D. Blondel. „Unique in the Crowd: The privacy bounds of human mobility." *Scientific Reports*, 2013. http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html.

Naor, Moni, and Moti Yung. „Universal One-Way Hash Functions and their Cryptographic Applications." In *STOC*, 33-43. 1989.

Nguyen, Lan. „Accumulators from Bilinear Pairings and Applications." In *CT-RSA*, 275- 292. 2005.

Popa, Raluca Ada, Hari Balakrishnan, and Andrew Blumberg. „VPriv: protecting privacy in location-based vehicular services." In *USENIX Security Symposium*. 2009.

Popa, Raluca Ada, Andrew J Blumberg, Hari Balakrishnan, and Frank H Li. „Privacy and accountability for location-based aggregate statistics." In *ACM CCS*. 2011.

Research, Pike. Electric Vehicle Market Forecasts. http://www. pikeresearch . com /research/electric-vehicle-market-forecasts, 2013. Accessed January 29, 2013.

Sampigethaya, K., Mingyan Li, Leping Huang, and R. Poovendran. „AMOEBA: Robust Location Privacy Scheme for VANET." *IEEE Journal on Selected Areas in Communications* 25, no. 8 (October 2007): 1569-1589. issn: 0733-8716. doi:10.1109/JSAC.2007.071007.

Shokri, R., G. Theodorakopoulos, J. Le Boudec, and J. Hubaux. „Quantifying Location Privacy." In 2011 *IEEE Symposium on Security and Privacy* (SP). May 2011. doi:10.1109/SP.2011.18.

Stegelmann, Mark, and Dogan Kesdogan. „Design and Evaluation of a Privacy-Preserving Architecture for Vehicle-to-Grid Interaction." In *EuroPKI*. 2012.

A Implementation Details

The current source code is a makefile project, written in C. We chose the language C, as the external routines and the libraries we rely on are also written in C, hence the whole project and its dependencies are written in one language. We implemented XSGS as a library. This XSGS library uses the GNU Multiple Precision Arithmetic Library1[42] for the basic arithmetic operations, the Pairing-Based Cryptography Library2[43] (PBC) for the curve and pairing-based arithmetic operations, the optimized reference implementation of the authors for the SHA3 hash algorithm (Keccak3) and the OpenSSL Library4 for RSA signature and certificate support.

[42] https://gmplib.org/
[43] https://crypto.stanford.edu/pbc/

At compile time one can choose between the TCMalloc Library[44] for a fast and multithreaded malloc() or the GNU C Library memory allocation, which will be linked to the XSGS library.

B Cryptographic parameters

The PBC library defines a variety of pairing types, of which our XSGS implementation uses either type D, F, or G, respectively. The type can be chosen at compile time. The group order is ~300 bits, the curve parameters are as follows: r >= 160, q >=1024/k, k= 6 (type D) 12 (type F) 10 (type G).

Where Paillier's operations are used, the modulus is of 1024 bit; RSA can by chose at compile time to use key lengths of either 1024, 2048, or 4096. The cryptographic hash function used throughout the XSGS implementation is the SHA3 contest winner Keccak with 256 bit hash length.

[44] https://code.google.com/p/gperftools/