TPP: Traceable Privacy-preserving Communication and Precise Reward for Vehicle-to-Grid Networks in Smart Grids

Huaqun Wang, Bo Qin, Qianhong Wu, *Member, IEEE*, Li Xu, and Josep Domingo-Ferrer, *Fellow, IEEE*

Abstract—In vehicle-to-grid (V2G) networks, service providers are battery-powered vehicles (BVs) and the service consumer is the power grid. Security and privacy concerns are major obstacles for V2G networks to be extensively deployed. In 2011, Yang *et al.* proposed a very interesting privacy-preserving communication and precise reward architecture for V2G networks in smart grids. In this paper, we enhance Yang *et al.*'s framework with formal definitions of unforgeability and restrictiveness. Then, we propose a new traceable privacy-preserving communication and precise reward scheme with available cryptographic primitives. The proposed scheme is formally proven secure with well-established assumptions in the random oracle model. Thorough theoretical and experimental analyses demonstrate that our scheme is efficient and practical for secure V2G networks in smart grids.

Index Terms—Secure communication, smart grid, V2G networks, privacy protection.

1 Introduction

A smart grid is a digitally enabled electrical grid that gathers, distributes, and acts on information about the behavior of all participants (suppliers and consumers) in order to improve the efficiency, importance, reliability, economics, and sustainability of electricity services. Smart grids have drawn great attention in both industry and academia. A vehicle-to-grid (V2G) network is a system in which plug-in electric or hybrid vehicles communicate with the power grid to sell services on-demand by either delivering electricity into the grid or by throttling their charging rate [1, 2]. Since most vehicles are parked 95% of the time on average, their batteries could be used to let electricity flow from the car to the power lines and back, with a value to the utilities of up to $4,000 per year per car [3]. We denote these plug-in electric vehicles as battery vehicles or BVs. V2G networks can bring lots of benefits to the power grid, for example, smoothing the variable generation capacity of renewable sources, distributed grid-connected storage for unexpected outages, faster response time, new ancillary services, etc. Many trial projects for V2G networks have already been deployed around the world [4–6].

- *H. Wang is with the School of Information Engineering, Dalian Ocean University, the State Key Laboratory of Integrated Services Networks, Xidian University and State Key Laboratory of Information Security, and Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China. E-mail: wanghuaqun@aliyun.com*
- *B. Qin is with the School of Information, Renmin Univeristy of China, China. E-mail: qinboo@xaut.edu.cn*
- *Q. Wu is with the School of Electronics and Information Engineering, Beihang University, China. E-mail: qhwu@xidian.edu.cn*
- *L. Xu is with the College of Mathematics and Computer Science, Fujian Normal University, China. E-mail: xuli@fjnu.edu.cn*
- *J. Domingo-Ferrer is with Universitat Rovira i Virgili, Dept. of Computer Engineering and Maths, UNESCO Chair in Data Privacy, Av. Països Catalans 26, E-43007 Tarragona, Catalonia. E-mail: josep.domingo@urv.cat*

1.1 Motivation

Security and privacy concerns are among the main obstacles for V2G networks to be extensively deployed. In order to provide services to the power grid, V2G network operators need to monitor the current status of each BV (location, battery capacity, battery state of charge, time to live, etc.). In this way, they can evaluate the total electricity storage capacity that is currently available. After collecting the current status of BVs, V2G network operators can provide service to the smart grid. In V2G networks, the individual BVs are the ones who provide ancillary services to the power grid; hence, the service paradigm is one of multiple service providers (individual BVs) providing services to a single user (power grid) in return for respective rewards. In addition, in V2G networks, the service providers are the ones who need privacy protection during the monitoring and rewarding processes. Privacy protection and rewarding can encourage more BVs to participate in the V2G network. In order to thwart improper BV behavior, traceability is also a prerequisite. When a BV improperly requests a reward several times for a single service, its identity should be traceable. Thus, traceability, privacy preservation and

precise rewarding are relevant security properties for V2G networks which motivate our study of traceable and privacy-preserving (TPP) reward systems in the V2G setting.

1.2 Related Work

The research in V2G networks is still at an early stage. Most existing works [7–13] mainly focus on the design of conceptual structures or the impact of V2G networks on the current power grid. Recently, a few pioneering studies on privacy issues in V2G networks in smart grids have appeared. Stegelmann *et al.* discussed an adversary algorithm based on travel times and showed how to obtain anonymity sets for individual vehicles [14]. Almost at the same time, they also studied the location privacy for V2G interaction through battery management [15]. By proposing an anonymous payment system with privacy protection support, Liu *et al.* provided the mechanisms to enhance location privacy of electric vehicles [16]. In 2013, Nicanfar *et al.* proposed a robust privacy-preserving authentication scheme for communication between the electric vehicles and the station to prevent customer information leakage [17]. In 2014, Rottondi *et al.* proposed a security infrastructure for privacy-friendly V2G interactions [18, 19]. In [14–19], the researchers contributed solutions to ensure identity and location privacy for the BVs.

Practical deployment needs further improvement of the existing schemes. For one thing, the incentives to BVs for V2G interaction have received little attention. Furthermore, there is no traceability mechanism to identify misbehaving BVs. Also, in vehicle communications, balancing trustworthiness, safety and BV privacy is a relevant design goal [20]. A prominent contribution came from Yang *et al.* [21] who proposed a very interesting privacy-preserving communication and precise reward architecture for V2G networks. They proposed a type of precise and equitable incentive model with better usability, where the operator of a V2G network rewards each participating BV for each service it provides. This incentive model does not require BV owners to sign a long-term contract or obey restricted connection times, thus giving the BV owners great freedom to use their own BVs. Those authors made the first attempt to address privacy considering the very specific nature of V2G networks.

1.3 Our Contribution

This paper further investigates the vital security and privacy issues of V2G networks in smart grids. Our starting point is Yang *et al.*'s privacy-preserving communication and precise reward architecture. Their instantiated scheme relies on Chen *et al.*'s ID-based restrictive partially blind signature technique [22]. Unfortunately, Chen *et al.*'s scheme does not satisfy the property of restrictiveness (see [23]) and then the generated *permit* is also forgeable. Therefore, the critical *permit* credential to access the V2G network can be generated without following the protocol, so that misbehaving BVs can use their *permit* credentials multiple times without revealing their own identities. We observe that this weakness is due to the lack of formal security definitions to capture realistic attacks in their reward architecture of V2G networks, and accordingly, to the lack of formal proofs to guarantee that their scheme is secure against potential attacks. In this paper, we fill this gap with formal definitions of unforgeability and restrictiveness in the security-enhanced reward architecture. We propose a new traceable privacy-preserving communication and precise reward scheme with available cryptographic primitives. The proposed scheme is formally proven secure with well-established assumptions in the random oracle model. Theoretical and experimental analyses demonstrate that our scheme is efficient and practical for secure V2G networks in smart grids.

1.4 Organization

The rest of this paper is organized as follows. Section 2 gives some cryptographic background; in particular, we introduce a new computational problem and prove its hardness. Section 3 introduces the system architecture and the security model. Section 4 presents our TPP scheme. Section 5 gives a detailed security and performance analysis of our proposal. Finally, Section 6 concludes the paper.

2 Background

In this section, we will review ID-based cryptography, bilinear pairings and restrictive partially blind signatures. When reviewing pairings, we introduce the new problem on whose difficulty the security of our scheme relies and we relate it to another problem of proven difficulty.

2.1 Identity-based cryptography and bilinear pairings

Identity-based cryptography (IBC) is a type of public-key cryptography in which a user's recognizable unique identity information is used as his/her public key. This identity-based feature eliminates the requirement of complicated public key certificates to certify each user's public key in traditional public key cryptosystems (PKC). Hence, IBC is better than PKC to secure systems in which the users' identities are recognizable. Most IBC schemes are built from bilinear pairings. We briefly introduce the bilinear pairing notion below.

Let $\mathcal{G}_1$ and $\mathcal{G}_2$, respectively, be a cyclic additive group generated by P and a cyclic multiplicative group with the same prime order q, *i.e.*, $|\mathcal{G}_1| = |\mathcal{G}_2| =$

q. Let $e : \mathcal{G}_1 \times \mathcal{G}_1 \rightarrow \mathcal{G}_2$ be a bilinear map, which satisfies the following properties:

1) Bilinearity: $\forall Q, R, S \in \mathcal{G}_1$ and $a, b \in Z$,
$$e(R, Q+S) = e(Q+S, R) = e(Q, R)e(S, R),$$
$$e(aR, bQ) = e(R, Q)^{ab}.$$
2) Non-degeneracy: $\exists Q, R \in \mathcal{G}_1$ such that $e(Q, R) \neq 1_{\mathcal{G}_2}$.
3) Computability: $\forall Q, R \in \mathcal{G}_1$, there is an efficient algorithm to calculate $e(Q, R)$.

Such a bilinear map e can be constructed using the modified Weil [24] or Tate pairings [25] on elliptic curves. A group with such a map e is called a bilinear group, on which the Computational Diffie-Hellman (CDH) problem is assumed hard while the Decisional Diffie-Hellman (DDH) problem is easy [26]. Namely, given unknown $a, b, c \in \mathcal{Z}_q$ and $P, aP, bP, cP \in \mathcal{G}_1$, it is known that there exists an efficient algorithm to determine whether $ab = c \bmod q$ by verifying $e(aP, bP) \stackrel{?}{=} e(P, cP)$ in polynomial time (DDH problem), while there exist no efficient algorithms to compute $abP \in \mathcal{G}_1$ with non-negligible probability within polynomial time (CDH problem). We will also use the following assumptions.

Assumption 1 ($\hat{q}$-Strong Diffie-Hellman Problem): ($\hat{q}$-SDH) [27] For a randomly chosen $a \in \mathcal{Z}_q^*$ and a random generator $P \in \mathcal{G}_1$ with order q, given $\hat{q}+1$ elements $(P, aP, a^2P, \cdots, a^{\hat{q}}P)$, it is difficult to compute a pair $(c, (c+a)^{-1}P) \in \mathcal{Z}_q \times \mathcal{G}_1$.

By using the bilinear pairing technique, the DDH problem is easy in the group $\mathcal{G}_1$. But the DDH problem remains difficult in other groups, such as $\mathcal{G}_2$. The security of our scheme relies on the difficulty of the n-linear representative pairing problem stated further below. The difficulty of this new problem will be shown to be related to the difficulty of the $(\bar{P}, \bar{Q}, \bar{f})$-DDH problem, introduced in [28] and recalled next.

Let s, n be positive integers. Let $\bar{P}, \bar{Q} \in \mathcal{Z}_q[X_1, X_2, \cdots, X_n]^s$ be two s-tuples of n-variate polynomials over $\mathcal{Z}_q$. Let $\bar{P}$ and $\bar{Q}$ be two sets of polynomials in $\mathcal{Z}_q[X_1, X_2, \cdots, X_n]$. The two sets are ordered, and write $p_1, p_2, \cdots, p_s$ and $q_1, q_2, \cdots, q_s$ for their elements, respectively. The first components of $\bar{P}, \bar{Q}$ satisfy $p_1 = q_1 = 1$.

Let $G \in \mathcal{G}_1$ be a generator of $\mathcal{G}_1$ and set $g' = e(G, G) \in \mathcal{G}_2$. We say that an algorithm $\mathcal{B}$ that outputs $b \in \{0, 1\}$ has advantage ϵ in solving the Decision $(\bar{P}, \bar{Q}, \bar{f})$- Diffie-Hellman problem [28] if

$$|\Pr[\mathcal{B}(p_1G, \cdots, p_sG, g'^{q_1}, \cdots, g'^{q_s}, g'^{f}) = 0] - Pr[\mathcal{B}(p_1G, \cdots, p_sG, g'^{q_1}, \cdots, g'^{q_s}, T) = 0]| > \epsilon$$

where the probability is over the random choice of generator $G \in \mathcal{G}_1$, the random choice of $x_1, \cdots, x_n$ in $\mathcal{Z}_q$, the random choice of $T \in \mathcal{G}_2$, and the random bits consumed by $\mathcal{B}$.

Definition 1: [28] Let $\bar{P}, \bar{Q} \in \mathcal{Z}_q[X_1, X_2, \cdots, X_n]^s$ be two s-tuples of n-variate polynomials over $\mathcal{Z}_q$. Write $\bar{P} = (p_1, p_2, \cdots, p_s)$ and $\bar{Q} = (q_1, \cdots, q_s)$ where $p_1 = q_1 = 1$. We say a polynomial $f \in \mathcal{Z}_q[X_1, \cdots, X_n]$ is dependent on the sets $(\bar{P}, \bar{Q})$ if there exist $s^2 + s$ constants $\{a_{i,j}\}_{i,j=1}^s$, $\{b_k\}_{k=1}^s$ such that

$$f = \sum_{i,j=1}^{s} a_{i,j} p_i p_j + \sum_{k=1}^{s} b_k q_k.$$

We say that f is independent of $(\bar{P}, \bar{Q})$ if f is not dependent on $(\bar{P}, \bar{Q})$.

For a polynomial $f \in \mathcal{Z}_q[X_1, \cdots, X_n]$, let d_f denote the total degree of f. For a set $\bar{P} \subseteq \mathcal{Z}_q[X_1, \cdots, X_n]^s$ we let $d_{\bar{P}} = max\{d_f | f \in \bar{P}\}$.

Theorem 1: [28] Let $\bar{P}, \bar{Q} \in \mathcal{Z}_q[X_1, \cdots, X_n]^s$ be two s-tuples of n-variate polynomials over $\mathcal{Z}_q$ and let $f \in \mathcal{Z}_q[X_1, \cdots, X_n]$. Let $d = max(2d_{\bar{P}}, d_{\bar{Q}}, d_f)$. If f is independent of $(\bar{P}, \bar{Q})$ then any $\mathcal{A}$ that has advantage $\frac{1}{2}$ in solving the decision $(\bar{P}, \bar{Q}, f)$-Diffie-Hellman Problem in a generic bilinear group $\mathcal{G}_1$ must take time at least $\Omega(\sqrt{q/d} - s)$.

Using the above theorem, we can get many standard (decisional) assumptions.

1) DDH in $\mathcal{G}_2$: set $\bar{P} = (1), \bar{Q} = (1, x, y)$, $f = xy$.
2) Bilinear Diffie-Hellman (BDH) in $\mathcal{G}_1$: set $\bar{P} = (1, x, y, z), \bar{Q} = (1)$, $f = xyz$.

The security of our scheme relies on the difficulty of the following n-Linear Representative Pairing Problem which is a computational (more difficult) version of the $(\bar{P}, \bar{Q}, f)$-DDH problem.

Assumption 2: (n-Linear Representative Pairing Problem (n-LRPP)): Given n random points $P_1 = \alpha_1 P, \cdots, P_n = \alpha_n P$ for some unknown $\alpha_i \in \mathcal{Z}_q$ and randomly chosen generator P of $\mathcal{G}_1$, and n pairing elements $(e(\Gamma, P_1), e(\Gamma, P_2), \cdots, e(\Gamma, P_n))$ for some secret point $\Gamma = rG \in \mathcal{G}_1 \backslash \{0\}$ and $\hat{P} = \alpha_{n+1} P \in \mathcal{G}_1$ for some $\alpha_{n+1} \in \mathcal{Z}_q$, it is difficult to compute a pair $e(\Gamma, \hat{P})$, where $\alpha_{n+1} \notin \{\sum_{i=1}^n a_i \alpha_i\}$ and $r \notin \{\sum_{i=1}^n a_i \alpha_i\}$ for all constants $a_1, a_2, \cdots, a_n \in \mathcal{Z}_q$.

We justify the hardness of the n-LRPP problem with the following statement.

Theorem 2: The n-Linear Representative Pairing Problem is hard if the $(\bar{P}, \bar{Q}, f)$-DDH problem is hard.

Proof: Denote $\bar{P} = \{1, \alpha_1, \cdots, \alpha_n, \alpha_{n+1}\}, \bar{Q} = \{1, r\alpha_1, \cdots, r\alpha_n\}$. $\bar{P}$ and $\bar{Q}$ can have the same number of elements by adding dummy elements.

Since r and Γ are secret, $r\alpha_{n+1}$ is independent of $\sum_{i,j=1}^{n+1} a_{i,j} \alpha_i \alpha_j$ from the attacker's viewpoint. Note the requirement $\alpha_{n+1} \notin \{\sum_{i=1}^n a_i \alpha_i\}$. We denote $\alpha_{n+1} = \sum_{k=1}^n b_k \alpha_k + a$ where $0 < a < min\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$. We get $r\alpha_{n+1} = \sum_{k=1}^n b_k (r\alpha_k) + ar$. Since $r \notin \{\sum_{i=1}^n a_i \alpha_i\}$ is unkown and $0 < a < min\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$, we have that $r\alpha_{n+1} \in \{\sum_{i=1}^n a_i \alpha_i\}$ holds only with negligible probability. Therefore, $f = r\alpha_{n+1}$ is independent of $(\bar{P}, \bar{Q})$. From Theorem 1, the following difference is negligible

$$|\Pr[\mathcal{B}(G, \alpha_1 G, \cdots, \alpha_{n+1} G, g'^{r\alpha_1}, \cdots, g'^{r\alpha_n}, g'^{r\alpha_{n+1}}) = 0] - \Pr[\mathcal{B}(G, \alpha_1 G, \cdots, \alpha_{n+1} G, g'^{r\alpha_1}, \cdots, g'^{r\alpha_n}, T) = 0]|$$

If our proposed n-linear representative pairing problem is easy, then $g'^{r\alpha_{n+1}} = e(\Gamma, \hat{P})$ can be calculated. Accordingly, the $(\bar{P}, \bar{Q}, f)$-DDH problem can be solved. From Theorem 1, the $(\bar{P}, \bar{Q}, f)$-DDH problem is difficult. Therefore, the n-Linear Representative Pairing problem is difficult and the corresponding n-LRPP assumption holds. □

2.2 Restrictive partially blind signatures

ID-based restrictive partially blind signatures are an important cryptographic tool for our concrete scheme. In 1982, Chaum introduced blind signatures, which allow a recipient to obtain a signature on message m without revealing anything about the message to the signer [29]. Blind signatures are used in applications where anonymity is of great concern, like electronic cash or electronic voting. Unfortunately, blind signatures cannot solve the double-spending problem in electronic cash schemes. In 1993, Brands introduced restrictive blind signatures which allow a recipient to receive a blind signature on a message unknown to the signer but the choice of the message is restricted and must conform to certain rules [30, 31]. Partially blind signatures were introduced by Abe and Fujisaki [32]. They allow a signer to produce a blind signature on a message for a recipient in such a way that the signature explicitly includes some commonly agreed visible information. In some cases, restrictiveness and partial blindness are absolutely necessary. Thus, Maitland and Boyd [33] first incorporated these two properties and proposed a provably secure restrictive partially blind signature scheme. Along with the development of bilinear pairings, ID-based restrictive partially blind signatures have attracted the interest of many researchers.

In 2007, Chen *et al.* first introduced the notion of ID-based restrictive partially blind signature and proposed a concrete signature scheme from bilinear pairings [22]. Regretfully, their scheme was shown insecure in [23]. After that, many ID-based restrictive partially blind signature schemes were designed, although some of them were found insecure [34–38]. In this paper, we design our TPP protocol by leveraging ID-based restrictive partially blind signatures as the tool [38]. The formal system model and the security definition are proposed in [22]. We omit them for the sake of conciseness.

ID-based restrictive partially blind signatures are an important cryptographic primitive that can be used in many fields, such as anonymous electronic payment. To the best of our knowledge, the existing schemes suffer from the following shortcomings: (1) lack of security; (2) inefficiency; (3) lack of a formal security proof. In order to overcome these shortcomings, we design a new *permit* generation scheme based on the idea of ID-based restrictive partially blind signature. Then, we give a formal security proof and an efficiency analysis.

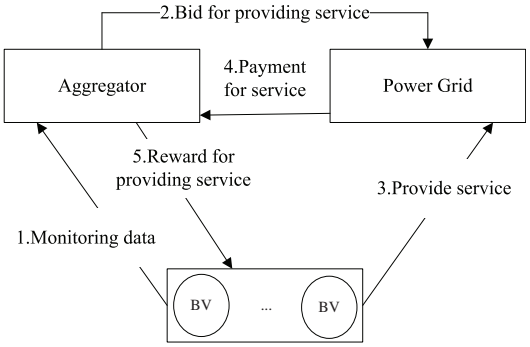


Fig. 1. V2G network model

3 System architecture and security model

In this section, we give the system architecture and security model for V2G networks in smart grids, mostly due to [21].

3.1 System architecture

In order to collect power from a large group of BVs and make transactions with the power grid, an aggregator is needed in the system architecture of V2G. At the same time, the aggregator can also be used to avoid the V2G network relying on the behavior of individual BVs during service provision. The system model is illustrated in Figure 1. BV sends monitoring data to the aggregator. The aggregator collects these monitoring data and evaluates the current total electricity storage capacity of all the BVs in the V2G network. Then, the aggregator makes bids in the electricity market. If successful, the aggregator selects a subset of BVs to provide the requested service. After confirming that the service has been completed, the power grid makes a payment to the aggregator and the aggregator rewards each BV that was selected to provide this service. Since the interaction between the aggregator and the power grid just follows the state of the art in electricity management, we only focus on the interaction between BVs and the aggregator. Specifically, we only focus on how to report monitoring data to the aggregator and how to reward individual BVs for providing services.

In the V2G network architecture, there are four parties, *i.e.*, the central aggregator (CAG), the local aggregators (LAGs), the individual BV, and a trusted authority (TA). Their roles can be described as follows:

1) CAG belongs to the operator of the V2G network and can directly communicate with the electricity market on behalf of the geographically dispersed BVs.
2) LAG also belongs to the operator of the V2G network, but it is deployed for each local area. LAG directly monitors every BV within this local

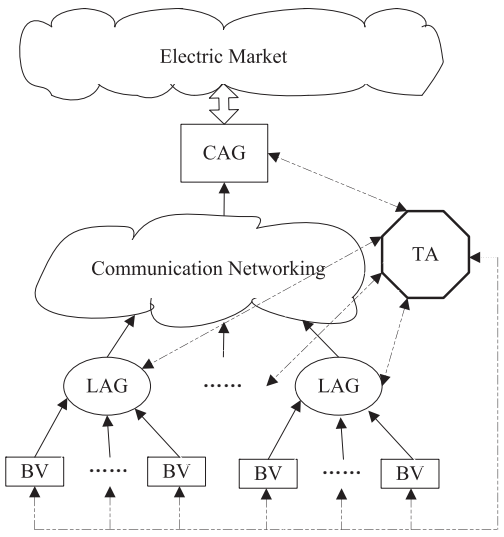


Fig. 2. V2G network architecture

area and sends the collected monitoring data to CAG in batch mode.

3) BV is in a commercial parking lot or a private residence. BV can connect to the power grid by deploying a charging device.
4) TA can be shared by multiple V2G networks. TA does the system initialization, like generating public system parameters, assigning a private key for each entity and so forth. It is trusted by all the other parties.

The network architecture of a V2G is depicted in Figure 2.

3.2 Security model

In this paper, the private information corresponds to the location and identity of each BV during its participation in the V2G network. In order to protect the privacy of BVs, the following security goals should be achieved:

1) Mutual authentication between BV and aggregator (CAG or LAG). Here mutual authentication means that a BV can verify that it is communicating with the expected aggregator and an aggregator can also be convinced that it is communicating with the expected BV. With mutual authentication, no attacker can impersonate a BV or an aggregator to cheat another party.
2) Confidentiality and integrity of the communication. Confidentiality implies that the communications are only readable to the intended receivers, which guarantees data privacy for the communicating parties. Integrity means that the receiver can verify whether the received data are identical to the data originated by the sender, which prevents an attacker from modifying or replaying messages to cheat the receivers.
3) Location and identity privacy of BV. It is required that no entity other than the BV can link its true identity with each parking location of the BV. This guarantees the location and identity privacy of the BVs.
4) Incontestable and anonymous reward. The BV owner should get a reward from aggregators that exactly corresponds to its contribution without revealing its true identity. However, if the BV owner redeems the same reward twice, the aggregator should be able to trace the true identity of this BV owner with the help of CAG. This achieves a practical balance between the privacy of the BVs and the functionality of the system. That is, an honest BV can stay anonymous but a misbehaving BV cannot.
5) Efficient revocation or enrollment. A mechanism should be provided to allow BVs to join or quit the V2G network efficiently.

The formal security definitions are given below:

Definition 2 (Restrictiveness): Let M be BV's account at the start of the traceable privacy-preserving communication and precise reward protocol for V2G networks in smart grids. Let M' be the blinded account after the protocol has finished. If, for any M and blinding transformation applied by BV, there exists an integer a such that $M' = aM$, then the protocol is said to satisfy restrictiveness.

Notes: In our protocol suite, BV sends its own account M to CAG. Through interaction between BV and CAG, BV can get the *permit* to use a blinded account M' which satisfies the property of restrictiveness, *i.e.*, there exists an integer a such that $M' = aM$.

Definition 3 (Unforgeability): The *permit* generation protocol is unforgeable if, for any (probabilistic polynomial time) adversary $\mathcal{A}$, the probability that $\mathcal{A}$ wins the following game is negligible:

1) Initialization: Generate the system parameters *params*. Generate the master secret/public key pairs: (*sk, pk*)$\leftarrow Init(1^k)$. Send the system parameters and the master public key *pk* to $\mathcal{A}$.
2) Oracle query and response: $\mathcal{A}$ adaptively makes a number of different queries. Each query can be one of the following:
   a) Hash query. $\mathcal{A}$ makes Hash function queries adaptively and gets the corresponding responses.
   b) Extract query. $\mathcal{A}$ makes the private key queries on the different identities $ID_1, \cdots, ID_n$ where $ID_{CAG} \notin \{ID_1, \cdots, ID_n\}$. Then, $\mathcal{A}$ gets the corresponding private keys.
3) Forgery: $\mathcal{A}$ can forge a valid *permit* on a new message $\bar{M}$ which is different from the message M' that has been signed by CAG and BVs.

TABLE 1
Notations and descriptions

Notations	Descriptions
ID_x	True identity of an entity x in the V2G network
PS_x	Pseudonym generated by a BV x based on ID_x
Q_x/Γ_x	Public/private key pair of BV x corresponding to its true identity ID_x
Q_{PS_x}/Γ_{PS_x}	Public/private key pair of BV x corresponding to its pseudonym PS_x
$Sig_{\Gamma_x}(M)$	ID-based signature on the message M using signer x's private key Γ_x
$E_k(M)$	Symmetric key encryption on message M using the shared secret key k
$HMAC_k(M)$	Hash-based message authentication code on message M using the shared secret key k
ST_x	Current status of the BV x
$H(M_1, \cdots, M_n)$	Hash value of the concatenation of $M_1, \cdots, M_n$ binary representations
q	The order of $\mathcal{G}_1$ and $\mathcal{G}_2$
$\hat{q}$	$\hat{q}$-SDH (Strong Diffie-Hellman problem)
t_i	i-th timestamp

In the above game, we say that $\mathcal{A}$ wins if

$$\Pr[\text{Verify}(permit, params) = \text{“}success\text{”}] \geq \frac{1}{p(k)}$$

where $p(k)$ is a polynomial of the security parameter k. In other words, the success probability must be non-negligible for an adversary $\mathcal{A}$ to win.

Note: In our protocol suite, the *permit* is generated by CAG and BV, who are assumed to do it honestly. This does not preclude a BV from behaving as an adversary at other moments.

The notations throughout this paper are listed in Table 1.

4 Design of an Efficient Privacy-Preserving Communication and Precise Reward Scheme

Inspired by Yang *et al.*'s original system architecture and security requirements [21], we formalize the definitions of unforgeability and restrictiveness in the security-enhanced reward architecture. Following the architecture and the definitions, we design a new permit generation scheme based on the idea of ID-based restrictive partially blind signature. A novel traceable privacy-preserving communication and precise reward scheme is designed by using available cryptographic primitives. We conduct thorough theoretical and experimental analyses. The analyses show that our proposal is efficient and practical for secure V2G networks in smart grids.

In order to achieve a secure and efficient scheme, which can realize privacy-preserving communication and precise reward for individual BVs in a V2G network, we employ standard security technologies including ID-based restrictive partially blind signatures, digital signatures, message authentication codes and symmetric encryption, together with time stamping to prevent replay attacks. Based on the same private key extraction technique as ours, Barreto *et al.* proposed a signature algorithm [39] that can be used in our scheme. Our design comprises four protocols: i) initialization; ii) *permit*-based access control and BV monitoring; iii) anonymous service provision and reward; and iv) BV revocation. They are described next.

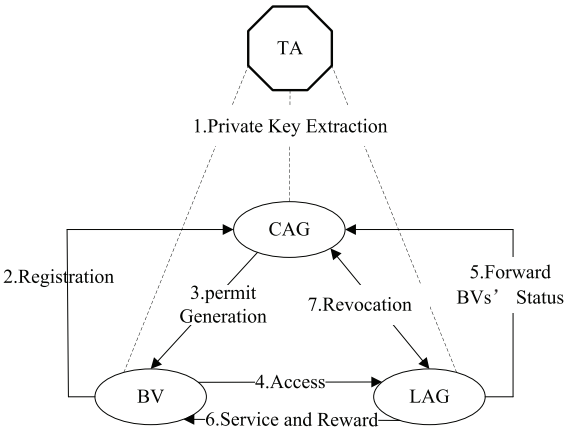


Fig. 3. Architecture of our TPP scheme

The architecture of our TPP scheme is given in Figure 3. There are four entities, TA, CAG, LAG and BV, whose interactions can be outlined as follows (circled numbers in the sequel correspond to numbers in Figure 3). ① TA generates the system parameters and the private keys of the entities BV, LAG and CAG, that will constitute their identities; this corresponds to the *Initialization* procedure described below. ② BV computes its unique account number and registers it at CAG. ③ Based on the idea of ID-based restrictive partially blind signature, CAG creates the *permit* on BV's account number and sends it to BV. ④ Making use of *permit*, BV can access LAG and require to provide the service. ⑤ LAG forwards BV's status to CAG. ⑥ BV provides the service and gets the reward. ⑦ When some BV needs to be revoked, CAG and LAG cooperate to revoke the BV.

4.1 Initialization

TA picks $s \in \mathcal{Z}_q^*$ and computes $P_{pub} = sP$. The system parameters $params = \{\mathcal{G}_1, \mathcal{G}_2, e, q, P, P_1, P_2, P_{pub}, H\}$ are published, where these parameters satisfy

$$e : \mathcal{G}_1 \times \mathcal{G}_1 \rightarrow \mathcal{G}_2,$$
$$H : \{0,1\}^* \rightarrow \mathcal{Z}_q^*.$$

Also, q denotes the order of $\mathcal{G}_1$ and $\mathcal{G}_2$, P is a generator, and P_1, P_2 are two random elements in $\mathcal{G}_1$.

Each entity x, including all the BVs, LAGs and CAG, submits its identity information, which can be represented by a unique string $ID_x \in \{0,1\}^*$, to TA to get its public/private key pair Q_x/Γ_x, where $Q_x = P_{pub} + H(ID_x)P \in \mathcal{G}_1^*$ and $\Gamma_x = (s + H(ID_x))^{-1}P$.

Each BV$_i$ randomly generates a number $u_i \in \mathcal{Z}_q^*$ and computes a unique account number $A_{BV_i} = u_iP_1 + P_2$. Then, BV$_i$ registers A_{BV_i} at CAG. Both ID_{BV_i} and A_{BV_i} will be stored at CAG and u_i will be kept as BV$_i$'s secret number.

In our scheme, in order to realize the confidentiality and authentication of the communication, ID-based encryption and signatures are required. Sometimes, message authentication techniques are also required. In order to simplify the description of our solution, we omit the concrete encryption and signature algorithms. Any secure and efficient ID-based encryption and signature algorithms can be used in our scheme. We clarify this by giving an example of the communication between BV and CAG. Suppose that BV sends the message M_1 to CAG in a secret and authenticated manner and CAG sends M_2 to BV with secrecy and integrity. We use Barreto *et al.*'s signature algorithm [39] as *Sig*. The symmetric key k_1 is generated below.

1) BV picks $r_1 \in \mathcal{Z}_q^*$ and computes
$$\bar{R}_1 = r_1(P_{pub} + H(ID_{CAG})P),$$
$$k_1 = e(P,P)^{r_1}.$$
Then, BV sends the following message to CAG:
$$\{ID_{BV}, \bar{R}_1, E_{k_1}\{M_1, t_1, \bar{R}_1, Sig_{\Gamma_{BV}}(ID_{BV}, M_1, t_1, \bar{R}_1)\}\}.$$
2) CAG computes $k_1 = e(\Gamma_{CAG}, \bar{R}_1)$ and decrypts the received ciphertext $E_{k_1}\{M_1, t_1, \bar{R}_1, Sig_{\Gamma_{BV}}(ID_{BV}, M_1, t_1, \bar{R}_1)\}$. It checks the validity of the signature $Sig_{\Gamma_{BV}}(ID_{BV}, M_1, t_1, \bar{R}_1)$. If it is valid, CAG accepts M_1 and sends the following message to BV:
$$E_{k_1}\{M_2, t_2, HMAC_{k_1}(M_2, t_2)\}.$$
3) BV decrypts the received ciphertext $E_{k_1}\{M_2, t_2, HMAC_{k_1}(M_2, t_2)\}$ and verifies its integrity by using $HMAC_{k_1}(M_2, t_2)$. If it is valid, BV accepts the message M_2.

The above instance gives a concrete communication solution which satisfies confidentiality, authentication and integrity. This solution can be used in the protocols specified in the rest of this paper, but we will omit it for the sake of conciseness.

4.2 Permit-based access control and BV monitoring

When a BV accesses the V2G network, the corresponding LAG asks it to present a *permit*. The *permit* is generated by CAG and assigned to the corresponding BV in advance. In the sequel, we describe the procedures for *permit* generation and *permit* verification. In the following procedures, t_i is a timestamp which is used to resist the replay attack.

4.2.1 Permit generation

In this procedure, *permit* is generated after five rounds of interaction between BV and CAG. Suppose M is the original message sent by BV to CAG for signing, and c is the agreed common information. Parameter c contains the expiration time of *permit* for BV's efficient revocation.

1) BV lets $M = A_{BV}$ and computes
$$g = e(P,P),\ g_1 = e(P_1, Q_{CAG}),\ g_2 = e(P_2, Q_{CAG}).$$
Then, BV sends the following message to CAG:
$$\{ID_{BV}, M, t_1\}.$$
2) Upon receiving $\{ID_{BV}, M, t_1\}$, CAG picks $r \in \mathcal{Z}_q^*$ and computes
$$R = g^r, R_1 = e(\Gamma_{CAG}, M), R_1' = R_1^r.$$
Then, CAG sends the following message to BV:
$$\{R, R_1, R_1', t_2\}.$$
3) Upon receiving $\{R, R_1, R_1', t_2\}$, BV picks $a, b, \alpha, \beta, \sigma_1, \sigma_2 \in \mathcal{Z}_q^*$ and computes
$$M' = aM,$$
$$U = R_1^a,$$
$$B = g_1^{\sigma_1} g_2^{\sigma_2},$$
$$T_1 = R^{\alpha} g^{\alpha\beta H(c)},$$
$$T_2 = R_1'^{a\alpha} U^{\alpha\beta H(c)},$$
$$p' = H(H(c), M', B, U, T_2, T_1),$$
$$p = \alpha^{-1}p' + \beta.$$
Then, BV sends $\{p, t_3\}$ to CAG.
4) Upon receiving $\{p, t_3\}$, CAG computes $V = (r + pH(c))\Gamma_{CAG}$ and sends $\{V, t_4\}$ to BV.
5) Upon receiving $\{V, t_4\}$, BV computes $V' = \alpha V$ and gets the final signature *permit*=$\{ID_{CAG}, M', c, U, B, p', V'\}$ on the message pair (M', c), where c is the agreed common information.

4.2.2 Permit verification

When BV accesses the V2G network, it presents *permit* and a pseudonym PS_{BV} to a LAG in the local area. BV generates the pseudonym by randomly selecting a number $\tilde{u} \in \mathcal{Z}_q^*$ and computes the corresponding public/private key pair as $Q_{PS_{BV}} = \tilde{u}Q_{BV}$ and $\tilde{\Gamma}_{BV} = \tilde{u}\Gamma_{BV}$. The pseudonym PS_{BV} is used to easily construct session keys for the frequent communication during the BV monitoring process. The *permit* verification can be described as follows.

1) BV sends the following message to LAG: $\{Q_{PS_{BV}}, permit, t_5\}$.
2) Upon receiving $\{Q_{PS_{BV}}, permit, t_5\}$, LAG computes $A = e(M', Q_{CAG})$, $d = H(A, B, Q_{LAG}, t_6)$ and sends $\{d, t_6\}$ to BV.

3) Upon receiving $\{d, t_6\}$, BV computes $r_1 = d(u_i a) + \sigma_1, r_2 = da + \sigma_2$ and sends $\{r_1, r_2, t_7\}$ to LAG, where u_i is chosen by the BV and it satisfies $A_{BV} = u_i P_1 + P_2$.
4) LAG checks whether

$$p' = H(H(c), M', B, U, e(V', M')U^{-p'H(c)}, e(V', P_{pub} + H(ID_{CAG})P)g^{-p'H(c)})$$

and

$$g_1^{r_1} g_2^{r_2} = e(M', Q_{CAG})^d B$$

hold. If they hold, *permit* is valid.

4.2.3 BV monitoring

After confirming the validity of *permit* and $Q_{PS_{BV}}$, the next monitoring cycle will be performed. BV reports its current status ST_{BV} to LAG. After collecting the status of all BVs in the local area, LAG forwards them to CAG in a batch. As ST_{BV} is identified by pseudonym PS_{BV}, neither LAG nor CAG can link the monitoring data with the true identity of the BV.

1) BV sends $\{Q_{PS_{BV}}, ST_{BV}, t_8\}$ to LAG.
2) Upon receiving $\{Q_{PS_{BV}}, ST_{BV}, t_8\}$, LAG sends the following message to CAG: $\{Q_{LAG}, ST_{BV}, t_9\}$.
3) CAG receives and stores the message record $\{Q_{LAG}, ST_{BV}, t_9\}$.

4.3 Anonymous service provision and reward

After receiving the monitoring data from LAGs, the CAG computes the electricity storage capacity currently available in the V2G network and makes bids in the electricity market for providing some services which are publicly requested by the power grid. If a bid is successful, CAG will ask LAGs to select a subset of BVs to provide the requested service. LAGs then send to each selected BV a service command $cmd_{service}$ separately. The procedures for anonymous service provision and reward are given below.

1) LAG sends the following message to BV:

$$\{PS_{BV}, ID_{LAG}, cmd_{service}, reward_{value}, t_9\}$$

where $reward_{value}$ denotes the reward value of this service.
2) When the BV is going to disconnect from the power grid, it requests a single value $reward$ from LAG based on the sum of the reward values during the parking period. Thus, BV sends $\{\sum reward_{value}, t_{10}\}$ to LAG.
3) LAG and BV execute the restrictive partially blind signature scheme presented as in the *permit* generation. Let $M_r = M'$ represent the original message sent by BV to CAG for signing and $c_r = \sum reward_{value}$ represent the agreed common information. $M'_r = \alpha_r M_r$ is the blinded message where α_r is the random number that BV selected in the *permit* generation phase. The $reward$ consists of $\{ID_{LAG}, (M'_r, c_r), (U_r, B_r, p'_r, V'_r)\}$.

When the BV owner wants to redeem the $reward$ at CAG, he presents the $reward$ and the identity of LAG to CAG. The BV owner calculates responses as $r_{1_r} = d_r(u_i \alpha \alpha_r) + \beta_r, r_{2_r} = d_r \alpha \alpha_r + \sigma_r$ which is similar as in the *permit* verification. CAG performs the verification algorithm. If successful, CAG accepts and stores this $reward$.

4.4 BV revocation

When some BV needs to be revoked, we consider two cases:

- *Case 1*. If LAG or CAG want to revoke BV, CAG can do it by rejecting this BV's new requests. Furthermore, as parameter c contains the expiration date, this BV will become invalid after this date.
- *Case 2*. When some BV requires to be revoked, CAG notifies all LAGs that all subsequent attempts to access the V2G network by using BV's *permit*s should be rejected and communicated to CAG. CAG may then take measures against malicious vehicles attempting such accesses.

5 Security Analysis and Performance Comparison

In this section, we give a comprehensive security analysis and performance comparison. According to this analysis, our scheme is secure and more efficient than Yang *et al.*'s scheme.

Why can our proposed protocol suite achieve security? First, we give the intuition. Then, we give the rigorous security proof. In our attack, the receiver can construct (z', a', b') without using the values (z, a, b) generated by BV. Thus, the receiver can construct M' without using the message M which is blinded in the protocol. On the other hand, in our improved protocol suite, the verification hash value p' is computed as the hash function of several arguments, some of which are functions of p' itself. In the verification, the signed M' is combined with p' through $e(V', M')U^{-p'H(c)}$. Then, $e(V', M')U^{-p'H(c)}$ is the input element of the hash value p'. The nesting and combination ensure the security of our protocol suite.

5.1 Security analysis

Theorem 3 (Correctness): If BV, CAG and LAG are honest and follow the proposed scheme, *permit* passes the verification and is accepted by LAG.

Proof: According to the procedures of permit generation and permit verification, we get

$$\begin{aligned} & e(V', M')U^{-p'H(c)} \\ = \; & e(\Gamma_{CAG}, M')^{\alpha r} e(\Gamma_{CAG}, M')^{p'H(c)+\alpha\beta H(c)} \\ & \times U^{-p'H(c)} \\ = \; & R_1'^{a\alpha} U^{\alpha\beta H(c)} \\ = \; & T_2; \end{aligned}$$

$$\begin{aligned} & e(V', P_{pub} + H(ID_{CAG})P)g^{-p'H(c)} \\ = \; & e(P,P)^{r\alpha}e(P,P)^{p'H(c)+\alpha\beta H(c)}g^{-p'H(c)} \\ = \; & R^{\alpha}g^{\alpha\beta H(c)} \\ = \; & T_1. \end{aligned}$$

The other elements come from CAG or BV. As our scheme assures integrity in the communication process, the other elements will not be changed. Thus,

$$\begin{aligned} p' \; = \; & H(H(c), M', B, U, e(V', M')U^{-p'H(c)}, \\ & e(V', P_{pub} + H(Q_{CAG})P)g^{-p'H(c)}) \end{aligned}$$

holds. On the other hand,

$$\begin{aligned} & g_1^{r_1}g_2^{r_2} \\ = \; & e(r_1P_1 + r_2P_2, Q_{CAG}) \\ = \; & e((d(u_ia) + \sigma_1)P_1 + (da + \sigma_2)P_2, Q_{CAG}) \\ = \; & e(da(u_iP_1 + P_2), Q_{CAG})e(\sigma_1P_1 + \sigma_2P_2, Q_{CAG}) \\ = \; & e(M', Q_{CAG})^dB. \end{aligned}$$

Thus, our scheme satisfies correctness. □

Theorem 4 (Restrictiveness): Based on the difficulty of n-LRPP, the signed M' has the form $M' = aM$, where $a \in \mathcal{Z}_q^*$.

Proof: We prove this theorem for two cases: M is a generator and M is not a generator. For the first case, any signed M' has the form $M' = aM$, since M is a generator.

To prove the second case, we will proceed by contradiction. Assume that BV produces the signed message M'. M' can be expressed as $M' = \bar{a}M + \bar{a}'P$ where P is the generator of the group $\mathcal{G}_1$. If there exists $\hat{a} \in \mathcal{Z}_q^*$ that satisfies $\bar{a}'P = \hat{a}M$, then the theorem follows. Assume that such an $\hat{a}$ does not exist, and that CAG and LAG are honest and strictly perform our proposed protocol. Thus, CAG can respond all kinds of *permit* queries by BVs since it has its own private key Γ_{CAG}. On the other hand, the final signature $\{ID_{CAG}, M', c, U, B, p', V'\}$ on the message pair (M', c) can pass the *permit* verification, where c is the agreed common information. Then, according to the proof of Theorem 3, since the forged *permit* can pass the verification, we get

$$\begin{aligned} & e(V', M')U^{-p'H(c)} = T_2, \\ & e(V', M') = T_2U^{p'H(c)}, \\ & e(\alpha(r + pH(c))\Gamma_{CAG}, \bar{a}M + \bar{a}'P) = T_2U^{p'H(c)}, \end{aligned}$$

i.e., the following formula holds

$$\begin{aligned} & e(\Gamma_{CAG}, M)^{\bar{a}\alpha(r+pH(c))}e(\Gamma_{CAG}, \alpha(r + pH(c))\bar{a}'P) \\ = \; & T_2U^{p'H(c)}, \end{aligned}$$

$$\begin{aligned} & R_1'^{\bar{a}\alpha}e(\Gamma_{CAG}, M)^{\bar{a}\alpha pH(c)}e(\Gamma_{CAG}, \alpha(r + pH(c))\bar{a}'P) \\ = \; & T_2U^{p'H(c)}. \end{aligned}$$

Then, we can get

$$\begin{aligned} & e(\Gamma_{CAG}, \alpha(r + pH(c))\bar{a}'P) \\ = \; & T_2U^{p'H(c)}R_1'^{-\bar{a}\alpha}e(\Gamma_{CAG}, M)^{-\bar{a}\alpha pH(c)} \\ = \; & T_2U^{p'H(c)}R_1'^{-\bar{a}\alpha}R_1^{-\bar{a}\alpha pH(c)}. \end{aligned}$$

Let $P^* = \alpha(r + pH(c))\bar{a}'P$. Since $\bar{a}'P$ is not a multiple of M and H is a cryptographic hash function, with non-negligible probability P^* is not a multiple of M either. From the above formula, BV can get $e(\Gamma_{CAG}, P^*)$ where Γ_{CAG} is unknown to BV. This violates the assumption on the difficulty of the n-LRPP problem (Assumption 2). Hence, our proposed scheme satisfies restrictiveness. □

Theorem 5 (Unforgeability): If an attacker can forge a valid *permit* with probability $\epsilon \geq \frac{7Q}{2^k}$ within time bound T, where k is a security parameter and Q is the number of queries to the random oracle, then within time $T' \leq \frac{16QT}{\epsilon}$ and with probability $\epsilon' \geq \frac{1}{9}$, the challenger can solve the $\hat{q}$-SDH problem. Based on the difficulty of the $\hat{q}$-SDH problem, the signed *permit* is unforgeable.

Proof: This theorem will be proven by contradiction. Assume that there exists an attacker who can forge the *permit*; then there exists another algorithm which solves the $\hat{q}$-SDH problem. According to the cryptographic assumption that the $\hat{q}$-SDH problem is difficult, no attacker exists who can forge the *permit*. The detailed proof is given below.

Let $\mathcal{A}$ be an adversary who can forge a valid signature. We construct a challenger algorithm $\mathcal{C}$ which can solve the $\hat{q}$-SDH problem. On input $(P, \alpha P, \alpha^2 P, \cdots, \alpha^{\hat{q}} P)$, $\mathcal{C}$'s aim is to output the pair $(c, \frac{1}{c+\alpha}P)$. $\mathcal{C}$ simulates the adversary $\mathcal{A}$'s environment.

Initialization: $\mathcal{C}$ picks $w_1, w_2, \cdots, w_{\hat{q}-1} \in \mathcal{Z}_q$ and creates the polynomial $f(z) = \prod_{i=1}^{\hat{q}-1}(z + w_i) = \sum_{i=0}^{\hat{q}-1} c_i z^i, c_i \in \mathcal{Z}_q^*$. It calculates $H = \sum_{i=1}^{\hat{q}-1} c_i(\alpha^i P) = f(\alpha)P$ and $H_{pub} = \sum_{i=1}^{\hat{q}} c_{i-1}(\alpha^i P) = \alpha H$. (α, H_{pub}) is the system's master secret/public key pair. On the other hand, for $1 \leq i \leq \hat{q} - 1$, $\mathcal{C}$ calculates the polynomials $f_i(z) = \frac{f(z)}{z+w_i} = \sum_{i=0}^{\hat{q}-2} d_{i-1}z^i$ and $\sum_{i=0}^{\hat{q}-2} d_{i-1}\alpha^i P = f_i(\alpha)P = \frac{f(\alpha)}{\alpha+w_i}P = \frac{1}{\alpha+w_i}H$. Thus, $\mathcal{C}$ can obtain the pairs $(w_i, \frac{1}{\alpha+w_i}H), 1 \leq i \leq \hat{q} - 1$.

Oracle query and response:

1) H: $\mathcal{C}$ creates the tables L_1, L_2 and L_3, which are initialized empty.
   a) Identity query: On input $ID_i, 1 \leq i \leq \hat{q} - 1$, if $ID_i \neq ID_{CAG}$, $\mathcal{C}$ outputs w_i and stores (ID_i, w_i) in table L_1; if $ID_i = ID_{CAG}$, $\mathcal{C}$ picks $w^* \in \mathcal{Z}_q^*$ and outputs w^*. It stores (ID_{CAG}, w^*) in table L_1.
   b) General query: On input $Q_i = (r_{i1}, r_{i2}, r_{i3}, r_{i4}, r_{i5}, r_{i6}) \in \mathcal{Z}_q^* \times \mathcal{G}_1 \times \mathcal{G}_2^4$, $\mathcal{C}$ picks $h_i \in \mathcal{Z}_q^*$ and stores (Q_i, h_i) in L_2. Then, it outputs h_i.
   c) Common information query: On input the common information *info*, $\mathcal{C}$ picks $\hat{c} \in \mathcal{Z}_q^*$ and stores $(info, \hat{c})$ in L_3. Then, it outputs $\hat{c}$.
2) Extract: On input $ID_i \neq ID_{CAG}$, $\mathcal{C}$ retrieves (ID_i, w_i) and outputs $\frac{1}{\alpha+w_i}H$ which has been obtained in the Initialization above.

Forgery: According to the assumption in the theorem, the attacker $\mathcal{A}$ can forge a valid signature $\{ID_{CAG}, M', c, B, U, p', V'\}$. Thus, it can pass the verification, *i.e.*

$$\begin{aligned} p' &= H(H(c), M', B, U, e(V', M')U^{-p'H(c)}, \\ & \quad e(V', P_{pub} + H(ID_{CAG})P)g^{-p'H(c)}). \end{aligned}$$

We take H as the random oracle. According to the forking lemma [40], with the same random tape and with probability $\epsilon' \geq \frac{1}{9}$ within the time bound $T' \leq \frac{16QT}{\epsilon}$, the attacker can obtain another valid signature $\{ID_{CAG}, M', c, B, U, \hat{p}', \hat{V}'\}$ based on the same message and random tape. Then, we have

$$\begin{aligned} & e(V', P_{pub} + H(ID_{CAG})P)g^{-p'H(c)} \\ = \; & e(\hat{V}', P_{pub} + H(ID_{CAG})P)g^{-\hat{p}'H(c)}, \end{aligned}$$

i.e.,

$$\begin{aligned} & e(V' - \hat{V}', P_{pub} + H(ID_{CAG})P) \\ = \; & e(P, (p'H(c) - \hat{p}'H(c))P). \end{aligned}$$

We can get

$$(s + H(ID_{CAG}))(V' - \hat{V}') = (p' - \hat{p}')H(c)P,$$

i.e.,

$$\frac{1}{s + H(ID_{CAG})}P = [(p' - \hat{p}')H(c)]^{-1}(V' - \hat{V}').$$

From the simulation, $\mathcal{C}$ knows that $H(ID_{CAG}) = w^*$ from the table L_1. Then, $\mathcal{C}$ can get

$$\frac{1}{s + w^*}P = [(p' - \hat{p}')H(c)]^{-1}(V' - \hat{V}').$$

Finally, $\mathcal{C}$ gets the pair $(w^*, \frac{1}{\alpha + w^*}P)$. This solves the $\hat{q}$-SDH problem. Based on the difficulty of this problem, *permit* is unforgeable. □

Theorem 6 (Traceability): If a BV uses *permit* twice, BV's identity can be traced.

Proof: If *permit* has been used twice, during its two verification processes, CAG can get two pairs of responses from the corresponding LAG, respectively:

$$\begin{aligned} & r_1 = d(au_i) + \sigma_1, \; r_2 = da + \sigma_2, \\ & r_1' = d'(au_i) + \sigma_1, \; r_2' = d'a + \sigma_2. \end{aligned}$$

By making use of the two response pairs, CAG can deduce the secret number $u_i = \frac{r_1 - r_1'}{r_2 - r_2'}$ of the BV that has been used in this *permit*. Then, CAG can obtain the unique account number of the BV by computing $A_{BV} = u_i P_1 + P_2$. Finally, the malicious BV's true identity is revealed. □

On the other hand, as we adopt the restrictive partially blind signature technique and pseudonym, the LAG who verified the *permit* cannot deduce BV's true identity. Further, for each pair of *permit* and pseudonym, a BV only uses it within a single parking period, hence LAGs cannot link a specific BV's multiple activities. Thus, the location and identity privacy of the individual BV owner during the monitoring process is well protected. Of course, according to Theorem 6, if a BV uses *permit* twice, BV's identity can be traced. This assures that the reward is incontestable.

We now analyze the security of the communications among BV, CAG and LAG. In order to simplify our solution with ID-based encryption and signature algorithms, we leave out the concrete encryption algorithm, signature algorithm and message authentication techniques in the concrete procedures. Any efficient and secure encryption, signature and message authentication technique can be applied into our scheme. We gave an instance in Section 4.1 above. When two entities must communicate, they first run a key agreement protocol and generate a symmetric session key. Using the generated session key and a symmetric encryption algorithm, the two entities can secretly communicate. When the exchanged message needs authentication, we make use of the secure signature scheme [39], a message authentication technique (*e.g.*, keyed cryptographic hash function) and a timestamp. In this way, our scheme can ensure mutual entity authentication, as well as confidentiality and validity of the communication. The timestamp is used to prevent replay attacks.

5.2 Performance comparison

In this section, we analyze the performance of our scheme in terms of computation and final *permit* size. Both in Yang *et al.*'s scheme and our scheme, the most expensive operations are bilinear pairing (denoted as C_{par}), point multiplication (denoted as C_{mul}) and point addition (denoted as C_{add}). So, we only consider the computational cost of these three operations. Finally, we compare the size of the final signature.

5.2.1 Performance Table

Performance figures are given in Table 2. For BV monitoring, our scheme incurs no bilinear pairing, point multiplication or point addition cost, because k_2' can be obtained by a key-evolving technique. On the other hand, Yang *et al.*'s scheme incurs 1 bilinear pairing and 1 point multiplication cost for BV monitoring. For BV revocation, LAG or CAG incur only a small computational cost. The corresponding computational cost is not shown in Table 2. For *permit* generation, in our scheme we add digital signatures and message authentication codes in order to ensure authentication, integrity checking and secure communication. Digital signatures and MACs are also used in Yang *et al.*'s scheme, so we omit them in the comparison. Thus, Table 2 focuses on computations other than the ones mentioned in this paragraph when comparing the *permit* generation and *permit* verification costs between Yang *et al.*'s scheme and our scheme. It can be seen from the comparison that our scheme is more efficient than Yang *et al.*'s.

TABLE 2
Performance comparison

Scheme		Yang *et al.*	Our scheme
permit Generation	BV	$6C_{par} + 9C_{mul} + 4C_{add}$	$4C_{par} + 3C_{mul} + 1C_{add}$
	CAG	$4C_{par} + 5C_{mul} + 2C_{add}$	$2C_{par} + 1C_{mul}$
permit Verification	BV	$1C_{par} + 2C_{mul}$	$1C_{par} + 2C_{mul} + 1C_{add}$
	LAG	$7C_{par} + 1C_{mul} + 1C_{add}$	$5C_{par} + 1C_{mul} + 1C_{add}$
Final *permit* Size		$5\mathcal{G}_1^* + 2\mathcal{G}_2^* + 1\mathcal{Z}_q^* + \|c\|$	$3\mathcal{G}_1^* + 2\mathcal{G}_2^* + 1\mathcal{Z}_q^* + \|c\|$

5.2.2 Implementation

We implemented our scheme and Yang *et al.*'s scheme on the same platform, in order to demonstrate the effectiveness of our scheme. We used the C programming language with the GMP (GMP-5.0.5), Miracl and PBC (pbc-0.5.13) libraries. In the implementation, CAG and LAG ran on a laptop computer with the following features:

- CPU: Intel Core i7-3517U @ 1.90GHz
- Physical Memory: 4GB DDR3 1600MHz
- OS: Ubuntu 13.04 Linux 3.8.0-19-generic SMP i686

BV ran on a laptop with the following features:

- CPU: CPU I PDC E6700 3.2GHz
- Physical Memory: DDR3 2G
- OS: Ubuntu 11.10 over VMware-workstation-full-8.0.0

Our cryptographic choices were: i) an elliptic curve with 160-bit group order; ii) SHA-1 as the hash message authentication code; and iii) AES (Advanced Encryption Standard) as the symmetric encryption algorithm. We compared the performance of our scheme and Yang *et al.*'s scheme. Figure 4 depicts the comparison of BV's computational cost for *permit* generation. In the X-axis we represent the number n of generated *permits*. The Y-axis represents BV's computing time in ms (*i.e.*, milliseconds) in order to generate n *permits*. It can be observed that our scheme is more efficient than Yang *et al.*'s. Figure 5 depicts the comparison of CAG computational cost for *permit* generation. The X-axis represents the number n of generated *permits*. The Y-axis represents CAG's computing time (ms) to respond n *permit* queries. Our scheme is clearly more efficient than Yang *et al.*'s. Figure 6 depicts the comparison of BV's computational cost for *permit* verification. The X-axis represents the number n of verified *permits*. The Y-axis represents BV's computing time (ms) in order to verify n *permits*. It is easily observed that our scheme is almost as efficient as Yang *et al.*'s. Figure 7 depicts the comparison of LAG's computational cost for *permit* verification. The X-axis represents the number n of verified *permits*. The Y-axis represents LAG's computing time (ms) in order to verify n *permits*. Here also, our scheme is clearly more efficient than Yang *et al.*'s.

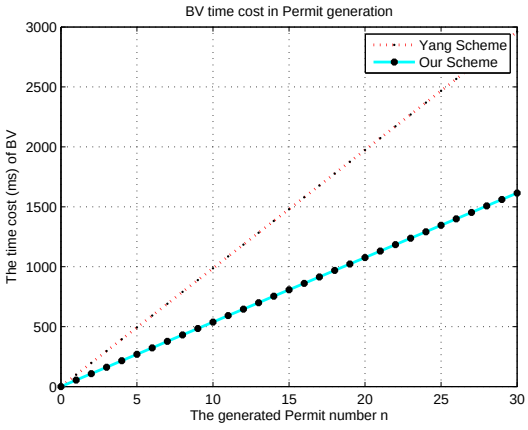


Fig. 4. BV's computing time (ms) as a function of the number of generated *permits*

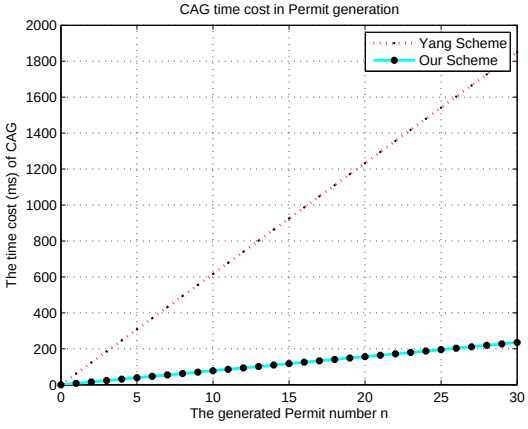


Fig. 5. CAG's computing time (ms) as a function of the number of generated *permits*

5.3 Resource Availability

If public key encryption is used in a straightforward way, end-to-end latency increases, which reduces resource availability. One can make use of the well-known digital envelope technique to address this problem. First, a pair of symmetric encryption/decryption algorithms (E, D) is agreed upon by sender and receiver, and the sender picks a random symmetric encryption key k for each message to be encrypted. Then, the sender encrypts the long message using E under k, and she encrypts k using the public key encryption algorithm under the receiver's public key. The sender sends the encrypted message and the encrypted k to the receiver, who recovers k by using his private key and then decrypts the long message using the symmetric decryption algorithm D under k. In this way, the use of public key en-

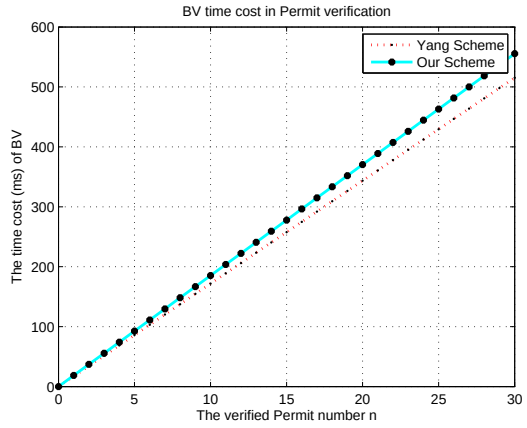


Fig. 6. BV's computing time (ms) as a function of the number of verified *permits*

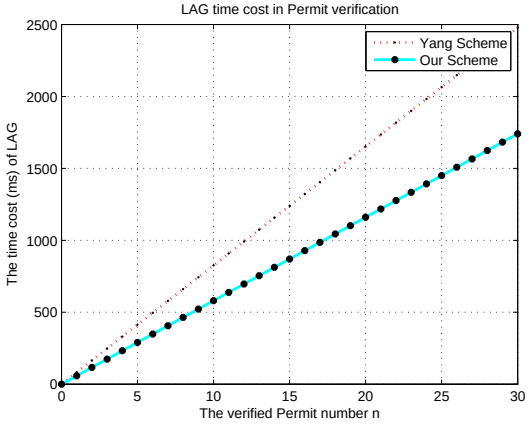


Fig. 7. LAG's computing time (ms) as a function of the number of verified *permits*

cryption/decryption and hence latency increase are minimized.

6 Conclusion

In this paper, we have revisited Yang *et al.*'s promising privacy protection and precise reward architecture for V2G networks in the smart grid. We pointed out a gap between their security model and their instantiated scheme, and we presented a new privacy-preserving and precise reward scheme with provable security in the random oracle model. We have shown that our scheme is superior in both security and efficiency.

Acknowledgments

The authors sincerely thank the editor for inviting competent referees, and the referees for their very valuable comments. This work was partly supported by the Natural Science Foundation of China through projects 61272522, 61370190 and 61173154, by the Natural Science Foundation of Liaoning Province through project 2014020147 and by the Program for Liaoning Excellent Talents in University through project LR2014021. The last author is with the UNESCO Chair in Data Privacy and he acknowledges support by the Government of Catalonia (grant 2014 SGR 537 and ICREA Acadèmia Award 2013), the Spanish Government (TIN2011-27076-C03-01 "CO-PRIVACY"), the European Commission (FP7 project "Inter-Trust" and H2020 project "CLARUS"), the Templeton World Charity Foundation (TWCF0095/AB60) and a Google Faculty Research Award. The views in this paper do not necessarily reflect the views of UNESCO or the Templeton World Charity Foundation.

References

[1] W. Kempton and J. Tomic, "Vehicle-to-grid power fundamentals: Calculating capacity and net revenue," *Journal of Power Sources*, vol. 144, no. 1, pp. 268-279, 2005.

[2] S. E. Letendre and W. Kempton, "The V2G concept: A new model for power?," *Public Utilities Fortnightly*, pp. 16-26, 2002.

[3] Car prototype generates electricity and cash, 2007 [Online]. Available: http://www.sciencedaily.com/releases/2007/12/071203133532.htm

[4] Smartgrid city [Online]. Available: http://smartgridcity.xcelenergy.com/

[5] Center for Carbon-Free Power Integration [Online]. Available: http://www.carbonfree.udel.edu/

[6] D. Graham-Rowe, "Denmark to power electric cars by wind in vehicle-to-grid experiment," London: *The Guardian*, June 19, 2009.

[7] C. Guille and G. Gross, "A conceptual framework for the vehicle-to-grid (V2G) implementation," *Energy Policy*, vol. 37, no. 11, pp. 4379-4390, 2009.

[8] S. Han, S. Han and K. Sezaki, "Development of an optimal vehicle-to-grid aggregator for frequency regulation," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 65-72, 2010.

[9] C. Quinn, D. Zimmerle and T. H. Bradley, "The effect of communication architecture on the availability, reliability, and economics of plug-in hybrid electric vehicle-to-grid ancillary services," *Journal of Power Sources*, vol. 195, no. 5, pp. 1500-1509, 2009.

[10] F. Kennel, D. Gorges and S. Liu, "Energy management for smart grids with electric vehicles based on hierarchical MPC," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 3, pp. 1528-1537, 2013.

[11] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati and G.P. Hancke, "A survey on smart grid potential applications and communication requirements," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 28-42, 2013.

[12] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati and G.P. Hancke, "Smart grid

technologies: communication technologies and standards," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 529-539, 2011.

[13] Smart Grid Cyber Security Strategy and Requirements, NIST Standard, Feb. 2010.

[14] M. Stegelmann and D. Kesdogan, "Design and evaluation of a privacy-preserving architecture for vehicle-to-grid interaction," *Public Key Infrastructures, Services and Applications*, LNCS 7163, pp. 75-90, 2012.

[15] M. Stegelmann and D. Kesdogan, "Location privacy for vehicle-to-grid interaction through battery management", *ITNG 2012*, pp. 373-378, 2012.

[16] J. Liu, M. Au, W. Susilo and J. Zhou, "Enhancing location privacy for electric vehicles (at the right time)", *ESORICS 2012*, LNCS 7459, pp. 397-414, 2012.

[17] H. Nicanfar, S. Hosseininezhad, P. TalebiFard and V. Leung, "Robust privacy-preserving authentication scheme for communication between electric vehicle as power energy storage and power stations", *INFOCOM 2013*, pp. 55-60, 2013.

[18] C. Rottondi, S. Fontana and G. Verticale, "Enabling privacy in vehicle-to-grid interactions for battery recharging", *Energies*, vol. 7, no. 5, pp. 2780-2798, 2014.

[19] C. Rottondi, S. Fontana and G. Verticale, "A privacy-friendly framework for vehicle-to-grid interactions", *SmartGridSec 2014*, LNCS 8448, pp. 125-138, 2014.

[20] Q. Wu, J. Domingo-Ferrer and Ú. González-Nicolás, "Balanced trustworthiness, safety and privacy in vehicle-to-vehicle communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp. 559-573, 2010.

[21] Z. Yang, S. Yu, W. Lou and C. Liu, "P^2: Privacy-preserving communication and precise reward architecture for V2G networks in smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 697-706, 2011.

[22] X. Chen, F. Zhang and S. Liu, "ID-based restrictive partially blind signatures and applications", *J. Syst. Softw*, vol. 80, no. 2, pp. 164-171, 2007.

[23] X. Hu and S. Huang, "Analysis of ID-based restrictive partially blind signatures and applications", *J. Syst. Softw*, vol. 81, pp. 1951-1954, 2008.

[24] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology-CRYPTO 2001*, LNCS 2139, pp. 213-229, 2001.

[25] A. Miyaji, M. Nakabayashi and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," *IEICE Transactions Fundamentals*, vol. 5, pp. 1234-1243, 2001.

[26] D. Boneh, B. Lynn and H. Shacham, "Short signatures from the Weil pairing," in *Advances in Cryptology-ASIACRYPT 2001*, LNCS 2248, pp. 514-532, 2001.

[27] D. Boneh and X. Boyen, "Short signatures without random oracles and the SDH assumption in bilinear groups," *Journal of Cryptology*, vol. 21, no. 2, pp. 149-177, 2008.

[28] D. Boneh, X. Boyen and E.-J. Goh, "Hierarchical identity based encryption with constant size ciphertext", *Advances in Cryptology-Eurocrypt 2005*, LNCS 3494, pp. 440-456, 2005. http://eprint.iacr.org/2005/015.pdf

[29] D. Chaum, "Blind signature for untraceable payments," *Advances in Cryptology-Eurocrypt 82*, Plenum Press, pp. 199-203, 1982.

[30] S. Brands, "Untraceable off-line cash in wallet with observers," *Advances in Cryptology-Crypto 1993*, LNCS 773, pp. 302-318, Springer, 1993.

[31] S. Brands, "An efficient off-line electronic cash system based on the representation problem," Technical Report CS-R9323, Centrum voor Wiskunde en Informatica (CWI), 1993.

[32] M. Abe and E. Fujisaki, "How to date blind signatures," *Advances in Cryptology-Asiacrypt 1996*, LNCS 1163, pp. 244-251, Springer, 1996.

[33] G. Maitland and C. Boyd, "A provably secure restrictive partially blind signature scheme," *PKC 2002*, LNCS 2274, pp. 99-114. Springer, 2002.

[34] G. Xu, "A new restrictive partially blind signature with designated verifier", *ICCSIT 2008*, pp. 123-126, 2008.

[35] X. Hu and S. Huang, "An efficient id-based restrictive partially blind signature scheme", *SNPD2007*, pp. 205-209, 2007.

[36] S. Wang, P. Han, Y. Zhang and X. Wang, "An improved id-based restrictive partially blind signature scheme", *SNPD2007*, pp. 295-300, 2007.

[37] C. Wang and R. Lu, "A certificateless restrictive partially blind signature scheme", *IIH-MSP 2008*, pp. 279-282, 2008.

[38] W. Cui, Y. Xin, C. Hu, Y. Yang and Z. Li, "Efficient ID-based (restrictive) partially blind signature", *Journal of Beijing University of Posts and Telecommunications*, vol. 31, no.4, pp. 53-57, 2008.

[39] P.S.L.M. Barreto, B. Libert, N. McCullagh and J.J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," *ASIACRYPT 2005*, LNCS 3788, Springer, pp. 515-532, 2005.

[40] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, No. 3, 2000, pp. 361-396.



Huaqun Wang received the BS degree in mathematics education from the Shandong Normal University and the MS degree in applied mathematics from the East China Normal University, both in China, in 1997 and 2000, respectively. He received the Ph.D. degree in Cryptography from Nanjing University of Posts and Telecommunications in 2006. Since then, he has been with Dalian Ocean University (China) as an associate professor. His research interests include applied cryptography, network security, and cloud computing security. He has published more than 40 papers. He has served in the program committee of several international conferences and the editor board of international journals.



Bo Qin received her Ph.D. degree in Cryptography from Xidian University in 2008 in China. Since then, she has been with Xi'an University of Technology (China) as a lecturer, and with Universitat Rovira i Virgili (Catalonia) as a senior researcher. Her research interests include pairing-based cryptography, data security and privacy, and VANET security. She has been a holder/co-holder of 5 China/Spain funded projects. She has authored over 50 publications and served in the program committee of several international conferences in information security.



Qianhong Wu received his his Ph.D. in Cryptography from Xidian University in 2004. Since then, he has been with Wollongong University (Australia) as an associate research fellow, with Wuhan University (China) as an associate professor, and with Universitat Rovira i Virgili (Catalonia) as a research director (research-only associate professor). His research interests include cryptography, information security and privacy, cloud computing security and *ad hoc* network security. He has been a holder/co-holder of 6 China/Australia/Spain funded projects. He has authored 5 patents and over 85 publications. He has served in the program committee of several international conferences and the editor board of ISI JCR. He is a member of IACR and IEEE.



Li Xu received the BS and MS degrees from the Fujian Normal University in 1992 and 2001, resp. He received the Ph.D. degree from the Nanjing University of Posts and Telecommunications in 2004. Now he is a Professor and Doctoral Supervisor in the School of Mathematics and Computer Science at the Fujian Normal University. He is also the Vice Dean of the School of Mathematics and Computer Science and the Director of the Key Lab of Network Security and Cryptography in Fujian Province. His interests include wireless networks and communications, network and information security, complex networks and systems, intelligent information in communication networks, etc. He has been invited to act as PC chair or member in more than thirty international conferences. He is a member of IEEE and ACM, and a senior member of CCF and CIE in China. He has published over 100 papers in journals and conferences.



Josep Domingo-Ferrer is a Distinguished Professor of Computer Science and an ICREA-Acadèmia Researcher at Universitat Rovira i Virgili, Tarragona, Catalonia, where he holds the UNESCO Chair in Data Privacy. His research interests are in data privacy and data security. He received his M. Sc. and Ph. D. degrees in Computer Science from the Autonomous University of Barcelona in 1988 and 1991, respectively. He also holds an M. Sc. in Mathematics. He has won several research and technology transfer awards, including twice the ICREA Academia Prize (2008 and 2013) and the "Narcís Monturiol" Medal to the Scientific Merit, both awarded by the Government of Catalonia, and a Google Faculty Research Award (2014). He has authored 5 patents and over 350 publications. He has been the coordinator of projects funded by the European Union and the Spanish government. He has been the PI of US-funded research contracts and currently of a Templeton World Charity Foundation grant. He has held visiting appointments at Princeton, Leuven and Rome. He is a co-Editor-in-Chief of *Transactions on Data Privacy*. He is an IEEE Fellow and an Elected Member of Academia Europaea.