

Role-Dependent Privacy Preservation for Secure V2G Networks in the Smart Grid

Hong Liu, *Student Member, IEEE*, Huansheng Ning, *Senior Member, IEEE*, Yan Zhang, *Senior Member, IEEE*, Qingxu Xiong, *Member, IEEE*, and Laurence T. Yang, *Member, IEEE*

Abstract—Vehicle-to-grid (V2G), involving both charging and discharging of battery vehicles (BVs), enhances the smart grid substantially to alleviate peaks in power consumption. In a V2G scenario, the communications between BVs and power grid may confront severe cyber security vulnerabilities. Traditionally, authentication mechanisms are solely designed for the BVs when they charge electricity as energy customers. In this paper, we first show that, when a BV interacts with the power grid, it may act in one of three roles: 1) energy demand (i.e., a customer); 2) energy storage; and 3) energy supply (i.e., a generator). In each role, we further demonstrate that the BV has dissimilar security and privacy concerns. Hence, the traditional approach that only considers BVs as energy customers is not universally applicable for the interactions in the smart grid. To address this new security challenge, we propose a role-dependent privacy preservation scheme (ROPS) to achieve secure interactions between a BV and power grid. In the ROPS, a set of interlinked subprotocols is proposed to incorporate different privacy considerations when a BV acts as a customer, storage, or a generator. We also outline both centralized and distributed discharging operations when a BV feeds energy back into the grid. Finally, security analysis is performed to indicate that the proposed ROPS owns required security and privacy properties and can be a highly potential security solution for V2G networks in the smart grid. The identified security challenge as well as the proposed ROPS scheme indicates that role-awareness is crucial for secure V2G networks.

Index Terms—Vehicle-to-grid (V2G), authentication, security, smart grid, privacy.

Manuscript received April 25, 2013; revised September 5, 2013; accepted December 6, 2013. Date of publication December 13, 2013; date of current version January 13, 2014. This work was supported in part by the National Natural Science Foundation of China, in part by the Civil Aviation Administration of China under Grant 61079019, in part by the National High-Tech Research and Development Program of China under Grant 2008AA04A101, in part by the European Commission FP7 Project EVANS under Grant 2010-269323, and in part by the SmartGrids ERA-Net project PRO-NET funded through Research Council of Norway under Project 217006. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Sen-Ching S. Cheung.

H. Liu and Q. Xiong are with the School of Electronic and Information Engineering, Beihang University, Beijing 100191, China (e-mail: liuhongler@ee.buaa.edu.cn; qxxiong@buaa.edu.cn).

H. Ning is with the School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100191, China, and also with the School of Electronic and Information Engineering, Beihang University, Beijing 100191, China (e-mail: ninghuansheng@buaa.edu.cn).

Y. Zhang is with the Simula Research Laboratory, Norway, and also with the Department of Informatics, University of Oslo, Norway (e-mail: yanzhang@simula.no).

L. T. Yang is with the School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China, and also with the Department of Computer Science, St. Francis Xavier University, Antigonish, NS B2G 2W5, Canada (e-mail: ltyang@stfx.ca).

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

Digital Object Identifier 10.1109/TIFS.2013.2295032

I. INTRODUCTION

THE smart grid is developing as the next-generation power infrastructure, in which bi-directional communications of electricity and information are established to achieve intelligent interactions. Particularly, smart grid enables customers and utilities to jointly participate in the management of power monitoring and dispatching for improving the demand-response balance [1], [2]. Vehicle-to-Grid (V2G) is an emerging network component in the smart grid, and has been received increasing attentions [3], [4]. In V2G networks, power transmission and communication are achieved by periodically collecting the energy status of a battery vehicle (BV), so that the BV can provide necessary information services for efficient power management. Additionally, geographically scattered BVs may be adopted as distributed electrical loads or energy resources to provide power services. During the interactions between BVs and the power grid, security vulnerabilities may be confronted due to the bi-directional communications. Thus, security and privacy issues become significant challenges in V2G networks. In this paper, we will identify and address a new security challenge in V2G networks owing to BVs' various interactions with the smart grid.

In V2G networks, a BV may play different roles, and accordingly has different responsibilities during interactions with the smart grid. It can be an entity to demand, store, or supply energy. Specifically, it may act as:

- *Energy Demand*: In this case, a BV acts as a consumer to require and charge electricity from the power grid. This is the traditional role of the BV in the smart grid. For the sake of illustration, we call such BV as a *load-BV*.
- *Energy Storage*: After a BV is charged, it can store the power in the battery. The BV becomes a distributed energy storage unit that may potentially provide electricity for the grid or other vehicles. In this case, we call the BV as a *storage-BV*.
- *Energy Supply*: A BV acts as a local power generator to provide energy support by feeding its stored power back to the power grid. The discharging operation is able to cut the load peaks and achieve demand response balance. In this sense, the BV acts as a Small Portable Power Plant (S3P) [5], [6]. Accordingly, we call the BV as a *S3P-BV*. The properly arranged S3P-BV may provide services to reduce operation cost and emission loss.

Fig. 1 shows a BV's individual privacy consideration when it acts as one of the roles. Revolving around a BV's different roles in V2G networks, dissimilar security and privacy chal-

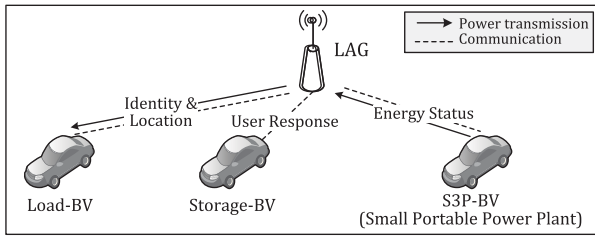


Fig. 1. BVs' roles in the smart grid and their privacy considerations.

lenges should be considered. For a load-BV, it accesses a local aggregator (LAG) as an energy customer to establish both power and communication links with the power grid. Before establishing the interactions, the load-BV and the LAG should perform mutual authentication to ensure the validity of identity. For a storage-BV, it has stored energy via the charging operation for future power utilization, and the BV may be challenged to participate in the discharging operation. Towards the storage-BV's response to the discharging request, the storage-BV has its own autonomy to decide its response (i.e., agree or decline). Here, the LAG cannot correlate the storage-BV's response with its real identity. For a S3P-BV, it performs the discharging operation to feed its stored power back to the grid. During the energy feeding, the LAG cannot obtain an individual energy status. It is observed that these security and privacy challenges are caused by the identity correlation related concerns. Traditionally, authentication mechanisms are solely designed for BVs when they charge electricity as energy customers. However, as we indicated, when a BV interacts with the power grid, it may act as one of three roles: energy demand (i.e., a customer), energy storage, and energy supply (i.e., a generator). In each role, the same BV has dissimilar privacy concerns and security requirements. Hence, the traditional approach that only considers BVs as energy customers is not universally applicable for the secure interactions between BVs and the grid. It is critical to design an anonymous authentication scheme to achieve privacy preservation for BVs, considering roles differentiation in the smart grid.

In this paper, we propose a role-dependent privacy preservation scheme (ROPS) for secure V2G networks in the smart grid. ROPS has considered the unique privacy concerns when a BV works in different roles. We also elaborate the situation when a BV works as an energy supplier by discharging electricity to the power grid. We propose that it may be implemented in two modes: centralized discharging and distributed discharging. In the centralized discharging operation, a BV will feed electricity to the central power grid, and then the grid can use the electricity for any purposes. In the distributed discharging operation, a BV does not feed electricity to the power grid, and it will discharge power to the local BVs under the same aggregator. Dissimilar authentication schemes are established to address these two discharging modes. Furthermore, we perform security analysis of the proposed scheme with respect to privacy preservation, session freshness, hierarchical access control, and data confidentiality and data integrity.

In summary, the objective of this paper is to propose a new authentication scheme to preserve privacy when a BV may act as different roles in the smart grid. To achieve this, we have three main contributions in this work.

- Identify a new security challenge in V2G networks, and address different privacy issues according to a BV's different roles as the energy demand, energy storage, and energy supply.
- Propose a role-dependent privacy preservation scheme to address the identified security challenge. In addition, we propose both centralized and distributed discharging operations for a S3P-BV for the central smart grid and the local neighboring load-BVs, respectively.
- Apply hybrid cryptographic primitives (e.g., ring signature, fair blind signature, and proxy re-encryption) to achieve anonymous authentication, and perform security analysis to demonstrate that the proposed scheme achieves security protection and privacy preservation.

The rest of this paper is organized as follows. Section II overviews the related work. Section III describes the system model, and we introduce both centralized discharging and distributed discharging modes when a BV feeds its power for energy supply. Section IV outlines the proposed ROPS authentication scheme. Section V discusses the inter-relationship of the sub-protocols in ROPS, and Section VI presents the security analysis. Finally, Section VII draws a conclusion.

II. RELATED WORK

There are few studies on the security and privacy issues in V2G networks. Yang *et al.* [7] identified privacy-preserving issues and proposed an innovative precise reward architecture. Concretely, a reward scheme P^2 was proposed to realize the trade-off between the participants' freedom of using the BVs and benefits provided by the operators. A secure communication architecture was proposed to achieve privacy preservation for BV monitoring and rewarding, in which an ID-based blind signature and an access control mechanism were introduced to realize anonymity authentication and hierarchical authority. Guo *et al.* [8] proposed a novel batch authentication protocol (UBAPV2G) to deal with multiple responses from a batch of vehicles. The proposed protocol introduces the concept of interval time for an aggregator verifying multiple vehicles, and applies the modified digital signature algorithm (DSA) algorithm to establish multiple object simultaneous verification. It turns out that such batch authentication mode has advantages comparing with the one-by-one authentication. Liu *et al.* [9] focused on different group attributes of BVs, and proposed an aggregated-proofs based privacy-preserving authentication scheme (AP3A) to achieve simultaneous identification and secure identification for BV's different working modes (i.e., home mode, and visiting mode). Moreover, Liu *et al.* [10] further proposed a battery status-aware authentication scheme (BASA) to address privacy preservation considering different battery status, including charging, fully-charged (FC), and discharging states. Three protocols were presented to guarantee the secure interaction between BVs and the power grid during the dynamic battery state transitions. Vaidya *et al.* [11]

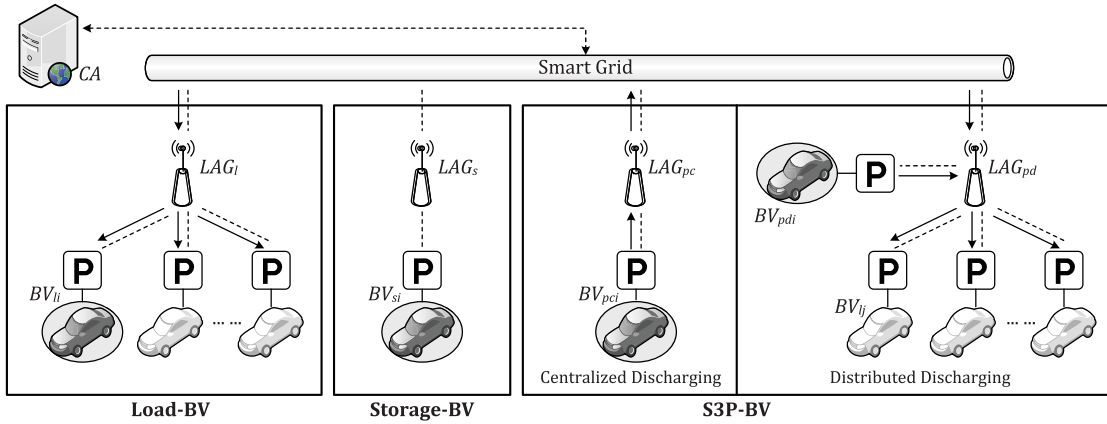


Fig. 2. The role-dependent system model in V2G networks.

proposed an original multi-domain network architecture for V2G networks. The scheme incorporates a comprehensive hybrid public key infrastructure (PKI) model which applies the peer-to-peer cross-certifications. Meanwhile, intra-domain management and inter-domain certificate management are established to achieve hierarchical access control. Tseng [12] proposed a secure and privacy-preserving communication protocol, which applies a blind signature and certificateless public key cryptography to achieve identity and location privacy perversion.

Our paper differs from these studies since we identify and solve a new security challenge in V2G networks. We observe that BVs may play different roles, including energy demand, storage, and supply. A BV has different privacy concerns when it works as different roles. Thus, a universal authentication scheme is not suitable for a BV. We need to design different authentication schemes for a BV that works in different roles, and further propose a new scheme to address the problem.

Additionally, several works have studied the general security issues in the smart grid, including security frameworks [13]–[19], authentication protocols [20]–[23], encryption and key management [24], [25], and privacy-preserving protocols [26], [27]. Li *et al.* [20] proposed a one-time signature based multicast authentication scheme, which is able to reduce storage cost and signature size compared with existing schemes, and is appropriate for lightweight applications. Fouda *et al.* [22] introduced a lightweight message authentication scheme, in which mutual authentication and the shared session keys are established by the hash-based authentication code and the Diffie-Hellman exchange protocol. Kim *et al.* [23] outlined a secure smart-metering protocol (SSMP) for power-line communication. Thereinto, the shared key transport protocol and meter-reading transmission protocol were designed without revealing any sensitive information, in which public-key encryption scheme is applied for the encryption. Lu *et al.* [27] reported a privacy-preserving aggregation scheme (EPPA), which applies a super-increasing sequence to structure multi-dimensional data and encrypt the structured data by the homomorphic Paillier algorithm. Meanwhile, the batch verification mode was adopted to reduce the authentication cost, and the proposed EPPA had high efficiency with

less computation and communication overhead. Our paper is different from these studies in two main aspects. First, we focus on the security and privacy issues in V2G networks instead of the generic smart grid. Second, the identified privacy problems related to BVs' different roles have not been studied yet in the literature.

III. SYSTEM MODEL

Fig. 2 illustrates a BV's role-dependent system model in V2G networks, which includes three main entities: battery vehicles (BVs), a local aggregator (LAG), and a central authority (CA). A BV is owned by an individual user and has a specific group attribute. LAG is granted by a power operator to collect BVs' energy status for power scheduling. CA as a trusted entity belongs to a nonaligned institution.

In the network model, BVs access the power grid for energy demand, and can also discharge the available power back into the smart grid. Thereinto, LAG directly communicates with the power grid on behalf of the geographically dispersed BVs, and acts as a power and information agent to establish power transmission and information communication. CA participates in all the communications, and can derive the detailed power and information data to support bill services, and the acquired data serves for the power grid management.

For the sake of presentation, we consider BV_i to introduce such role-dependent system. During BV_i 's accessing the power grid via LAG, it may act as three possible roles (i.e., load-BV, storage-BV, and S3P-BV). Revolving around the BV_i 's identity, dissimilar security and privacy requirements should be considered based on the different roles.

- **Load-BV:** $\{BV_{li}, LAG_l\}$ represent the variants of $\{BV_i, LAG\}$ as a load-BV and the corresponding aggregator. When BV_{li} accesses the power grid for energy demand, the power flows from the power grid into BV_{li} . Before performing the charging operation, $\{BV_{li}, LAG_l\}$ should establish mutual authentication to ascertain the validity of identity. BV_{li} should be verified without revealing its identity so that LAG_l cannot correlate BV_{li} 's sensitive identity with the location privacy.
- **Storage-BV:** $\{BV_{si}, LAG_s\}$ represent the variants of $\{BV_i, LAG\}$ as a storage-BV and the corresponding

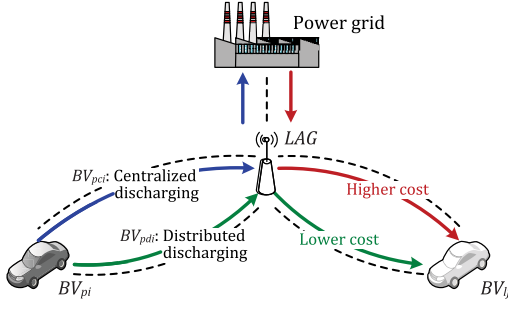


Fig. 3. The necessity of the centralized and distributed discharging modes.

aggregator. After completing the charging operation, BV_{si} becomes a potential energy source, and may be further challenged by CA to participant in the discharging operation for power-balance consideration. When BV_{si} receives the discharging request from CA , it may agree or decline the request. LAG_s can obtain the response to launch the corresponding operation, but cannot ascertain that the obtained response is from a specific BV_{si} to discover the user response privacy (e.g., the user may not want to perform the discharging operation, or may need to drive the BV immediately).

- **S3P-BV:** $\{BV_{pi}, LAG_p\}$ ($p \in \{pc, pd\}$) represent the variants of $\{BV_i, LAG\}$ as a S3P-BV and the corresponding aggregator. We define two types of energy supply modes for the S3P-BV, in which the subscripts $\{pc, pd\}$ are used to denote the centralized and distributed discharging operations, respectively. Thereinto, *centralized discharging* refers to the mode that BV_{pci} feeds its energy into the power grid for centralized energy dispatching. *Distributed discharging* refers to the mode that BV_{pdi} feeds its power to the neighboring load-BVs (BV_lj) for distributed energy utilization. The former mode is used for the case when there are no load-BVs in the local area, therefore the power can be returned into the grid for central dispatching. The latter mode is for the case when there are other load-BVs in the local area. The discharged electricity will be directly transmitted to the neighboring load-BVs for efficiency and cost considerations. In the two modes, the system has the following security requirements: 1) LAG_{pc} (LAG_{pd}) cannot correlate BV_{pci} 's (BV_{pdi} 's) identity with the energy status, 2) BV_l cannot correlate BV_{pdi} 's identity with the discharging status, and 3) BV_{pdi} or LAG_{pd} cannot correlate BV_l 's identity with the charging status.

It is beneficial to differentiate the centralized and distributed discharging modes for V2G networks, and Fig. 3 shows the necessity of the two discharging modes. Assume that a S3P-BV (i.e., BV_{pci} , or BV_{pdi}) performs energy supply for either power grid or neighboring load-BVs, the discharged energy can be regarded as non-difference. However, it is quite different towards the energy charged from the power grid and from its local BV_{pdi} considering the efficiency and cost, and BV_{pdi} 's neighboring load-BVs may enjoy more preferential electricity price during the distributed discharging operation

due to the lower transmission line losses. The distributed discharging mode can improve power scheduling efficiency, and avoid redundant power outflows and re-inflows.

In the system model, both power transmission (marked as the solid line) and information communication (marked as the dash line) are established between BVs and LAG. The arrows in the lines show the direction of power flow. For instance, BV_{li} as a load-BV performs charging operation, and the power flows from the power grid into the load-BV. BV_{si} is a storage-BV, and only a communication link is established among $\{BV_{si}, LAG_s, CA\}$. For BV_{pdi} as a S3P-BV working in the distributed discharging mode, its stored power flows into multiple BV_lj s via LAG_{pd} . In this case, there is less power transmission from the power grid.

Towards the attack model, the communication channels are exposed in public, and both internal and external attacks exist during interactions. The internal attacks mainly refer to the interactive legal entities. Thereinto, a LAG may be self-centered and utilitarian, and aims to obtain more BVs' private data contents and the associated user behaviors for the maximization of commercial interests; a BV may attempt to capture other BVs' sensitive data for certain purposes (e.g., curiosity, and malicious intent). The external attacks mainly consider the data CIA triad (i.e., confidentiality, integrity, and availability) threats from outside adversaries, which could compromise the legal entities, and subsequently perform data tampering or privacy disclosure. Concretely, the adversary may: corrupt and impersonate as a legal entity to forward and modify the intercepted messages in the current session; eavesdrop and record the exchanged messages in former sessions, and replay the messages in the ongoing communication; perform tracking and traffic analysis to monitor and estimate the user behaviors for passive aggressions. The adversary cannot: obtain the pre-shared secrets; extract the real identifier via the intercepted messages, or generate the consistent pseudonyms; acquire the pseudorandom generation algorithm.

IV. THE PROPOSED ROLE-DEPENDENT PRIVACY PRESERVATION SCHEME: ROPS

A. System Initialization

We consider BV_i to establish interactions with LAG , CA , and other BVs in V2G networks. Thereinto, BV_i are assigned with the pseudonyms $\{PID_{BV_i}, PID_{LAG}\}$, and LAG only has its own PID_{LAG} . Note that BV_i is defined in two types of groups during accessing the power grid: one is the *static group* that is assigned by a specific power operator, and the other is the *dynamic group* that is established by the temporarily gathered BVs around the same LAG 's range. Additionally, three hash functions are defined: $\{H_0, H_1\} : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$; $H_2 : \mathbb{Z}_q^* \times \mathbb{Z}_q^* \rightarrow \mathbb{Z}_q^*$, in which q is a large prime. The public key Y_τ ($\tau \in \{BV_i, LAG\}$) and the corresponding privacy key $x_\tau \in \mathbb{Z}_q^*$ are defined according to a generator $g \in \{0, 1\}^*$.

- For active entities (i.e., $\{BV_{\theta i}, LAG_{\theta}\}$, $\theta \in \{l, pc, pd\}$): $Y_{BV_i} = g^{x_{BV_i}} \pmod{p}$, and $Y_{LAG} = g^{x_{LAG}} \pmod{p}$.
- For inactive entities (i.e., $\{BV_{si}, LAG_s\}$): $Y'_{BV_i} = g^{x'_{BV_i}}$, and $Y'_{LAG} = g^{x'_{LAG}}$.

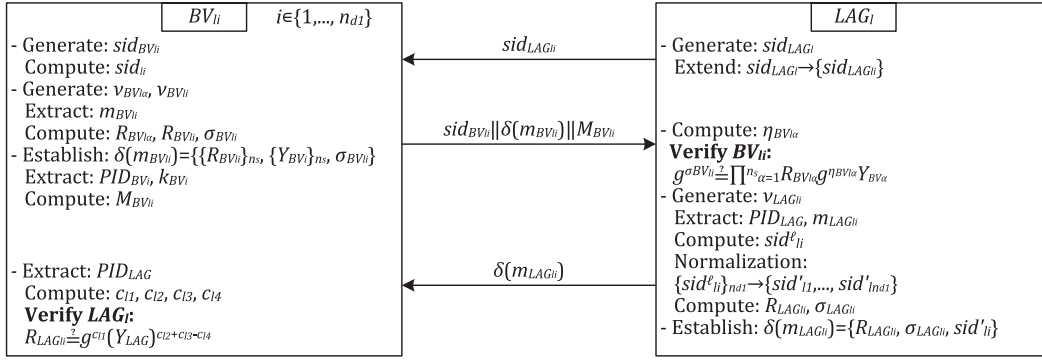


Fig. 4. LoadAP: The authentication protocol for the load-BV.

TABLE I
NOTATIONS

Notation	Description
BV_i	The i -th battery vehicle (BV). Note that BV includes battery electric vehicles, fuel cell vehicles, plug-in hybrid electric vehicles, etc [7].
LAG	The local aggregator.
CA	The central authority.
BV_{li}, BV_{si}	BV_i acting as a load-BV, and a storage-BV.
BV_{pci}, BV_{pdi}	BV_i acting as a S3P-BV in the centralized discharging mode and distributed discharging mode.
LAG_l, LAG_s	LAG connecting with BV_{li}, BV_{si} .
LAG_{pc}, LAG_{pd}	LAG connecting with BV_{pci}, BV_{pdi} .
PID_{BV_i}, PID_{LAG}	Pseudonym of BV_i, LAG .
sid_{BV_i}, sid_{LAG}	Session identifier of BV_i, LAG , attached with the entity group attribute.
$r_{BV_i}, r_{LAG}, r_{CA}$	Pseudorandom number of BV_i, LAG, CA .
$n_s/n'_s, n_{d^*}/n'_{d^*}$	The number of BVs in a static group and a dynamic group.
$\{Y_*, x_*\}$	The general symbols of the pairwise public key, and privacy key.
$\{\tilde{Y}_{BV_*}, \tilde{x}_{BV_*}\}$	The general symbols of a BV's pairwise pseudo public key, and pseudo privacy key.
k_{BV_i}	The individual key shared by BV_i and CA .
k_G, k_Σ	The group keys.
$E_k(\cdot), H(\cdot)$	The encryption, and hash function.
M^ℓ	The locally re-computed value M according to the same algorithm.
$\{M\}_{n_*}$	A set of values $\{M_1, \dots, M_{n_*}\}$.

Let $\mathbb{G} = \langle g \rangle$ denote that a group \mathbb{G} is generated based on g . There is a set of parameters $(q, g, f, \mathbb{G}, \mathbb{G}', e, H_1)$ in a bilinear map. Here, $\{\mathbb{G}, \mathbb{G}'\}$ are of prime order q , and $\langle g \rangle = \langle f \rangle = \mathbb{G}$. The mapping that $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}'$ satisfies the bilinear non-degenerate properties: i.e., for all $g \in \mathbb{G}$ and $a, b \in \mathbb{Z}_q^*$, it turns out that $e(g^a, f^b) = e(g, f)^{ab}$, and $e(g, f) \neq 1$. Note that full-fledged cryptographic algorithms (e.g., ring signature [28], blind signature [29], proxy re-encryption [30], and their variants) can be exploited to support the proposed ROPS. The main notations are listed in Table I.

B. LoadAP: Authentication Protocol for the Load-BV

Fig. 4 shows an interaction of $\{BV_{li}, LAG_l\}$. BV_{li} represents one of the load-BVs (i.e., $\{BV_{I1}, \dots, BV_{In_{d1}}\}$, $i \in \{1, \dots, n_{d1}\}$, $n_{d1} \in \mathbb{N}^*$), and BV_{li} accesses LAG_l along with

other load-BVs in a distributed way. Here, n_{d1} is the number of the BVs in BV_{li} 's temporarily dynamic group.

1) *Phase 1. LAG_l Challenging BV_{li}*: LAG_l generates a session identifier sid_{LAG_l} to initiate a new session. LAG further extends sid_{LAG_l} into $\{sid_{LAG_{li}}\}_{n_{d1}}$ (i.e., $\{sid_{LAG_{I1}}, \dots, sid_{LAG_{In_{d1}}}\}$) by Hamming distance based extension operation. Thereafter, LAG_l transmits $sid_{LAG_{li}}$ to BV_{li} as a challenge. Upon receiving the message, BV_{li} generates a session identifier $sid_{BV_{li}}$ to compute sid_{li} as a session-sensitive variable.

$$sid_{li} = H_0(sid_{BV_{li}} || sid_{LAG_{li}})$$

2) *Phase 2. LAG_l Verifying BV_{li}'s Ring Signature*: BV_{li} randomly chooses $v_{BV_{li}\alpha}$ and $v_{BV_{li}}$, in which $\alpha \in \{1, \dots, n_s\}$ and $\{v_{BV_{li}\alpha}, v_{BV_{li}}\} \in \mathbb{Z}_q^*$. Here, n_s refers to the number of BVs in BV_{li} 's affiliated static group, and $v_{BV_{li}\alpha}$ is a shading operator used to hide the proofs. Thereafter, BV_{li} extracts a message $m_{BV_{li}}$, and computes $R_{BV_{li}\alpha}$ ($\alpha \neq i$), and $R_{BV_{li}}$.

$$R_{BV_{li}\alpha} = g^{v_{BV_{li}\alpha}} \pmod{q}$$

$$R_{BV_{li}} = g^{v_{BV_{li}} - \sum_{\alpha=1, \alpha \neq i}^{n_s} H_2(H_1(m_{BV_{li}}), H_1(R_{BV_{li}\alpha}))}$$

$$\left(\prod_{\alpha=1, \alpha \neq i}^{n_s} Y_{BV_{li}\alpha} \right)^{-1} \pmod{q}$$

Thereafter, BV_{li} computes $\sigma_{BV_{li}}$, and establishes a ring signature $\delta(m_{BV_{li}}) = \{\{R_{BV_{li}}\}_{n_s}, \{Y_{BV_{li}}\}_{n_s}, \sigma_{BV_{li}}\}$.

$$\sigma_{BV_{li}} = v_{BV_{li}} x_{BV_{li}} + \sum_{\alpha=1, \alpha \neq i}^{n_s} v_{BV_{li}\alpha} + H_2(H_1(m_{BV_{li}}), H_1(R_{BV_{li}})) \pmod{q}$$

BV_{li} extracts the pseudonym $PID_{BV_{li}}$ and secret key $k_{BV_{li}}$ to compute $M_{BV_{li}}$. Here, $k_{BV_{li}}$ is a one-session available key shared by BV_{li} and CA . Thereafter, BV_{li} transmits $sid_{BV_{li}} || \delta(m_{BV_{li}}) || M_{BV_{li}}$ to LAG_l .

$$M_{BV_{li}} = E_{k_{BV_{li}}}(PID_{BV_{li}} \oplus sid_{li})$$

Upon receiving the message, LAG_l first computes $\eta_{BV_{li}} = H_2(H_1(m_{BV_{li}}), H_1(R_{BV_{li}\alpha}))$ ($\alpha \in \{1, \dots, n_s\}$) to verify BV_{li} by checking the following equation.

$$g^{\sigma_{BV_{li}}} \stackrel{?}{=} \prod_{\alpha=1}^{n_s} R_{BV_{li}\alpha} g^{\eta_{BV_{li}} Y_{BV_{li}}} \quad (1)$$

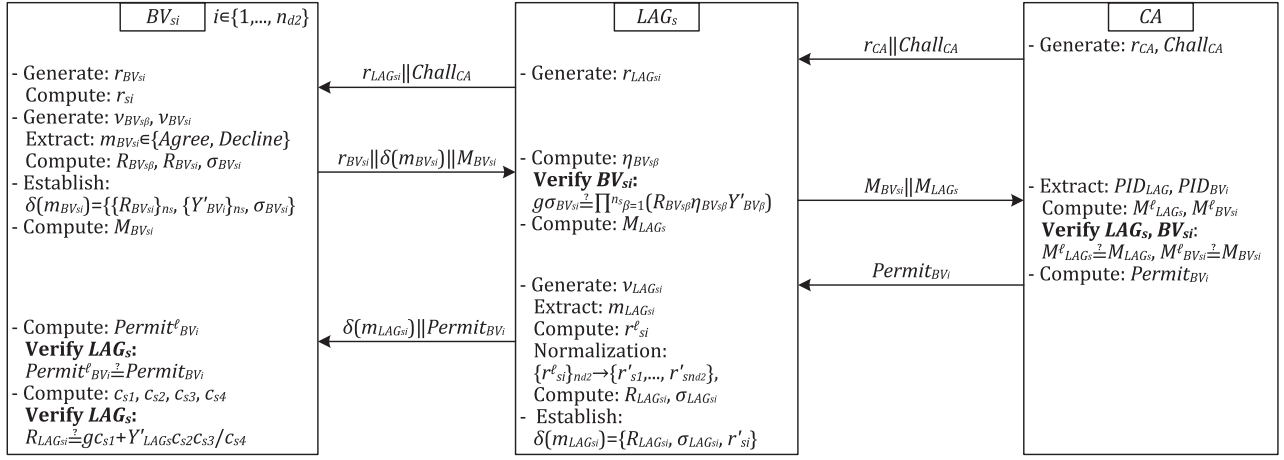


Fig. 5. StorageAP: The authentication protocol for the storage-BV.

- For the left side of (1), we have,

$$\begin{aligned} Left(1) &= g^{v_{BV_{li}}} g^{x_{BV_{li}}} g^{\sum_{\alpha=1, \alpha \neq i}^{n_s} v_{BV_{\alpha}}} g^{\eta_{BV_{li}}} \\ &= g^{v_{BV_{li}}} Y_{BV_{li}} \prod_{\alpha=1, \alpha \neq i}^{n_s} g^{v_{BV_{\alpha}}} g^{\eta_{BV_{li}}} \end{aligned}$$

- For the right side of (1), we have,

$$\begin{aligned} Right(1) &= R_{BV_{li}} g^{\eta_{BV_{li}}} Y_{BV_{li}} \prod_{\alpha=1, \alpha \neq i}^{n_s} R_{BV_{\alpha}} g^{\eta_{BV_{\alpha}}} Y_{BV_{\alpha}} \\ &= g^{v_{BV_{li}}} g^{\eta_{BV_{li}}} Y_{BV_{li}} g^{\sum_{\alpha=1, \alpha \neq i}^{n_s} v_{BV_{\alpha}}} \end{aligned}$$

If $Left(1) = Right(1)$ holds, LAG_l will regard BV_{li} as a legal load-BV, meanwhile LAG_l can only ascertain BV_{li} 's group information without obtain its specific identifier. Note that the maximum probability that LAG_l determines the identity of the actual signer BV_{li} is $1/n_s$.

3) *Phase 3. BV_{li} Verifying LAG_l 's Signature:* LAG_l randomly chooses $v_{LAG_{li}} \in \mathbb{Z}_q^*$, and extracts the pseudonym PID_{LAG} and a message $m_{LAG_{li}}$. LAG_l re-computes sid'_{li} , and normalizes $\{sid'_{li}\}_{n_{d1}}$ to obtain $\{sid'_{l1}, \dots, sid'_{ln_{d1}}\}$. Here, $\sum_{\alpha=1}^{n_{d1}} (sid'_{\alpha}) = H_0(PID_{LAG} || sid_{BV_{li}})$. LAG_l further computes $R_{LAG_{li}}$ and $\sigma_{LAG_{li}}$ for signature.

$$\begin{aligned} R_{LAG_{li}} &= g^{v_{LAG_{li}}} \pmod{q} \\ \sigma_{LAG_{li}} &= (v_{LAG_{li}})^{-1} (H_1(m_{LAG_{li}} || R_{LAG_{li}}) \\ &\quad + x_{LAG} (R_{LAG_{li}} + \sum_{\alpha=1, \alpha \neq i}^{n_{d1}} sid'_{\alpha})) \pmod{q} \end{aligned}$$

Thereafter, LAG_l establishes a signature $\delta(m_{LAG_{li}}) = \{R_{LAG_{li}}, \sigma_{LAG_{li}}, sid'_{li}\}$, and transmits it to BV_{li} for authentication. Upon receiving the message, BV_{li} extracts the pre-assigned pseudonym PID_{LAG} to compute a set of values $\{c_{l1}, c_{l2}, c_{l3}, c_{l4}\}$.

$$\begin{aligned} c_{l1} &= H_1(m_{LAG_{li}} || R_{LAG_{li}}) (\sigma_{LAG_{li}})^{-1} \pmod{q} \\ c_{l2} &= H_0(PID_{LAG} || sid_{BV_{li}}) (\sigma_{LAG_{li}})^{-1} \pmod{q} \\ c_{l3} &= R_{LAG_{li}} (\sigma_{LAG_{li}})^{-1} \pmod{q} \\ c_{l4} &= sid'_{li} (\sigma_{LAG_{li}})^{-1} \pmod{q} \end{aligned}$$

- BV_{li} verifies LAG_l by checking the following equation.

$$R_{LAG_{li}} \stackrel{?}{=} g^{c_{l1}} (Y_{LAG})^{c_{l2} + c_{l3} - c_{l4}} \quad (2)$$

- For the left side of (2), we have,

$$\begin{aligned} Left(2) &= g^{(\sigma_{LAG_{li}})^{-1} H_1(m_{LAG_{li}} || R_{LAG_{li}})} \\ &\quad g^{x_{LAG} (\sigma_{LAG_{li}})^{-1} (R_{LAG_{li}} + \sum_{\alpha=1, \alpha \neq i}^{n_{d1}} sid'_{\alpha})} \end{aligned}$$

- For the right side of (2), we have,

$$\begin{aligned} Right(2) &= g^{H_1(m_{LAG_{li}} || R_{LAG_{li}}) (\sigma_{LAG_{li}})^{-1}} \\ &\quad (Y_{LAG})^{(\sum_{\alpha=1}^{n_{d1}} (sid'_{\alpha}) + R_{LAG_{li}} - sid'_{li}) (\sigma_{LAG_{li}})^{-1}} \end{aligned}$$

If $Left(2) = Right(2)$ holds, BV_{li} will regard LAG_l as a legal aggregator, and $\{BV_{li}, LAG_l\}$ will establish mutual authentication without revealing BV_{li} 's identity information. LoadAP mainly considers BV_{li} 's location privacy preservation, in which a fixed LAG_l obtains BV_{li} 's group attribute, and cannot correlate the detailed location information with BV_{li} 's real identity.

After above mutual authentication, LAG_l further transmits $sid_{BV_{li}} || sid_{LAG_{li}} || M_{BV_{li}}$ to CA for identification and billing purposes. CA derives $PID_{BV_{li}}$ by encryption $E_{k_{BV_{li}}}^{-1} (M_{BV_{li}}) \oplus H_0(sid_{BV_{li}} \oplus sid_{LAG_{li}})$, therefore CA ascertains BV_{li} 's real identity. Generally, $\{LAG_l, CA\}$ are assigned hierarchical authorities on BV_i , i.e., LAG_l only knows BV_i 's general group attribute, and CA owns full authority on BV_i 's detailed identity.

C. StorageAP: Authentication Protocol for the Storage-BV

Fig. 5 shows an interaction of $\{BV_{si}, LAG_s, CA\}$, and BV_{si} as a storage-BV is a possible energy source to perform discharging for power dispatching. It has full autonomy to decide whether or not to participate in the discharging operation.

1) *Phase 1. CA Challenging $\{LAG_s, BV_{si}\}$:* CA generates a pseudorandom number r_{CA} , and a discharging request $Chall_{CA}$ to transmit $r_{CA} || Chall_{CA}$ to LAG_s . Afterwards,

LAG_s computes $r_{LAG_{si}}$, and transmits $r_{LAG_{si}} \parallel Chall_{CA}$ to BV_{si} .

$$r_{LAG_{si}} = H_0(sid_{LAG_{li}} \parallel r_{CA})$$

Upon receiving the message, BV_{si} generates a pseudorandom number $r_{BV_{si}}$ to compute r_{si} .

$$r_{si} = H_0(r_{BV_{si}} \parallel r_{LAG_{si}} \parallel sid_{li})$$

2) *Phase 2. LAG_s Verifying BV_{si} 's Ring Signature:* BV_{si} randomly chooses $\nu_{BV_{s\beta}}$ and $\nu_{BV_{si}}$, ($\beta \in \{1, \dots, n_s\}$, $\{\nu_{BV_{s\beta}}, \nu_{BV_{si}}\} \in \mathbb{Z}_q^*$). Thereafter, BV_{si} extracts the response message $m_{BV_{si}} \in \{Agree, Decline\}$, and computes $R_{BV_{s\beta}}$ ($\beta \neq i$), and $R_{BV_{si}}$.

$$\begin{aligned} R_{BV_{s\beta}} &= g\nu_{BV_{s\beta}} \pmod{q} \\ R_{BV_{si}} &= \nu_{BV_{si}} \left(\prod_{\beta=1, \beta \neq i}^{n_s} gH_2(H_1(m_{BV_{si}}), \right. \\ &\quad \left. H_1(R_{BV_{s\beta}}))Y'_{BV_{s\beta}} \right)^{-1} \pmod{q} \end{aligned}$$

Afterwards, BV_{si} computes $\sigma_{BV_{si}}$ to establish a ring signature $\delta(m_{BV_{si}}) = \{\{R_{BV_{si}}\}_{n_s}, \{Y'_{BV_{si}}\}_{n_s}, \sigma_{BV_{si}}\}$.

$$\begin{aligned} \sigma_{BV_{si}} &= \nu_{BV_{si}} H_2(H_1(m_{BV_{si}}), H_1(R_{BV_{si}}))x'_{BV_{si}} \\ &\quad \prod_{\beta=1, \beta \neq i}^{n_s} \nu_{BV_{s\beta}} \pmod{q} \end{aligned}$$

BV_{si} computes $M_{BV_{si}}$, and transmits the cascaded value $r_{BV_{si}} \parallel \delta(m_{BV_{si}}) \parallel M_{BV_{si}}$ to LAG_s .

$$M_{BV_{si}} = H_0(PID_{BV_{si}} \oplus r_{LAG_{si}})$$

Upon receiving the message, LAG_s computes $\eta_{BV_{s\beta}} = H_2(H_1(m_{BV_{si}}), H_1(R_{BV_{s\beta}}))$ ($\beta \in \{1, \dots, n_s\}$) to verify BV_{si} by checking the following equation.

$$g\sigma_{BV_{si}} \stackrel{?}{=} \prod_{\beta=1}^{n_s} (R_{BV_{s\beta}} \eta_{BV_{s\beta}} Y'_{BV_{s\beta}}) \quad (3)$$

- For the left side of (3), we have,

$$Left(3) = g\nu_{BV_{si}} \eta_{BV_{si}} x'_{BV_{si}} \prod_{\beta=1, \beta \neq i}^{n_s} \nu_{BV_{s\beta}}$$

- For the right side of (3), we have,

$$\begin{aligned} Right(3) &= R_{BV_{si}} \eta_{BV_{si}} Y'_{BV_{si}} \prod_{\beta=1, \beta \neq i}^{n_s} R_{BV_{s\beta}} \eta_{BV_{s\beta}} Y'_{BV_{s\beta}} \\ &= \nu_{BV_{si}} \eta_{BV_{si}} Y'_{BV_{si}} \prod_{\beta=1, \beta \neq i}^{n_s} \nu_{BV_{s\beta}} \end{aligned}$$

If $Left(3) = Right(3)$ holds, LAG_s will regard BV_{si} as a legal storage-BV, and LAG_l can only ascertain BV_{si} 's group attribute without obtaining the detailed identity information.

3) *Phase 3. CA Verifying $\{LAG_s, BV_{si}\}$:* LAG_s computes M_{LAG_s} , and transmits $M_{BV_{si}} \parallel M_{LAG_s}$ to CA for authentication.

$$M_{LAG_s} = H_0(PID_{LAG} \oplus r_{CA})$$

CA extracts the stored pseudonyms $\{PID_{LAG}, PID_{BV_{si}}\}$ to re-compute $M_{LAG_s}^{\ell}$ and $M_{BV_{si}}^{\ell}$ according to r_{CA} and $\{sid_{BV_{li}}, sid_{LAG_{li}}\}$. CA verifies $\{LAG_s, BV_{si}\}$ by checking whether $M_{LAG_s}^{\ell} = M_{LAG_s}$ and $M_{BV_{si}}^{\ell} = M_{BV_{si}}$ hold. If LAG_s is regarded as an illegal aggregator, the protocol will terminate; and if BV_{si} is regarded as an illegal storage-BV, the protocol will eliminate BV_{si} from the authentication. Thereafter, CA computes and transmits a certification $Permit_{BV_{si}}$ to LAG_s for assigning an access authority on BV_{si} .

$$Permit_{BV_{si}} = H_0(PID_{BV_{si}} \oplus PID_{LAG} \oplus Chall_{CA})$$

4) *Phase 4. BV_{si} Verifying LAG_s :* LAG_s randomly chooses numbers $\nu_{LAG_{si}}$ for $\nu_{LAG_{si}} \in \mathbb{Z}_q^*$, and re-computes r_{si}^{ℓ} . LAG_s obtains the normalized values $\{r_{si}^{\ell}\}_{n_{d2}} = \{r'_{s1}, \dots, r'_{sn_{d2}}\}$. Here, $\prod_{\beta=1}^{n_{d2}} (r'_{s\beta}) = H_0(PID_{LAG} \parallel r_{BV_{si}})$, and n_{d2} is the real-time number of the BVs in BV_{si} 's temporarily dynamic group. LAG_s computes $R_{LAG_{si}}$ and $\sigma_{LAG_{si}}$ to establish a signature of $m_{LAG_{si}}$.

$$\begin{aligned} R_{LAG_{si}} &= g\nu_{LAG_{si}} \pmod{q} \\ \sigma_{LAG_{si}} &= \nu_{LAG_{si}} (H_1(m_{LAG_{si}} \parallel R_{LAG_{si}}) \\ &\quad + x'_{LAG} R_{LAG_{si}} \prod_{\beta=1, \beta \neq i}^{n_{d2}} r'_{s\beta})^{-1} \pmod{q} \end{aligned}$$

LAG_s establishes $\delta(m_{LAG_{si}}) = \{R_{LAG_{si}}, \sigma_{LAG_{si}}, r'_{si}\}$, and transmits $\delta(m_{LAG_{si}}) \parallel Permit_{BV_{si}}$ to BV_{si} for authentication. Thereafter, BV_{si} re-computes $Permit_{BV_{si}}^{\ell}$ by its locally stored $\{PID_{LAG}, PID_{BV_{si}}\}$, and preliminarily verifies LAG_s by checking whether $Permit_{BV_{si}}^{\ell}$ equals $Permit_{BV_{si}}$. If it holds, LAG_s will perform further verification by computing a set of values $\{c_{s1}, c_{s2}, c_{s3}, c_{s4}\}$.

$$\begin{aligned} c_{s1} &= H_1(m_{LAG_{si}} \parallel R_{LAG_{si}}) \sigma_{LAG_{si}} \pmod{q} \\ c_{s2} &= H_0(PID_{LAG} \parallel r_{BV_{si}}) \sigma_{LAG_{si}} \pmod{q} \\ c_{s3} &= R_{LAG_{si}} \sigma_{LAG_{si}} \pmod{q} \\ c_{s4} &= r'_{si} \sigma_{LAG_{si}} \pmod{q} \end{aligned}$$

BV_{si} verifies LAG_s by checking the following equation.

$$R_{LAG_{si}} \stackrel{?}{=} gc_{s1} + Y'_{LAG} c_{s2} c_{s3} (c_{s4})^{-1} \quad (4)$$

- For the left side of (4), we have,

$$\begin{aligned} Left(4) &= g\sigma_{LAG_{si}} (H_1(m_{LAG_{si}} \parallel R_{LAG_{si}}) \\ &\quad + x'_{LAG} R_{LAG_{si}} \prod_{\beta=1, \beta \neq i}^{n_{d2}} r'_{s\beta}) \\ &= g\sigma_{LAG_{si}} H_1(m_{LAG_{si}} \parallel R_{LAG_{si}}) \\ &\quad + Y'_{LAG} \sigma_{LAG_{si}} R_{LAG_{si}} \prod_{\beta=1, \beta \neq i}^{n_{d2}} r'_{s\beta} \end{aligned}$$

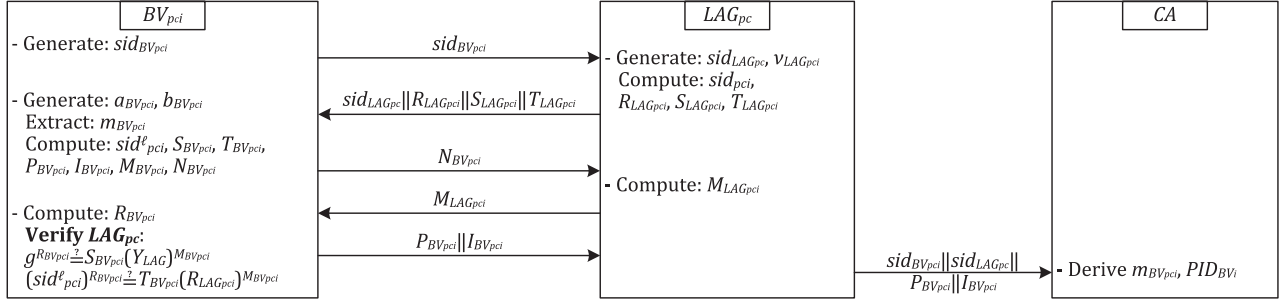


Fig. 6. S3PAP-C: The authentication protocol for the S3P-BV in the centralized discharging mode.

- For the right side of (4), we have,

$$\begin{aligned} Right(4) &= gH_1(m_{LAG_{si}} || R_{LAG_{si}}) \sigma_{LAG_{si}} \\ &+ Y'_{LAG} \prod_{\beta=1}^{n_{d2}} (r'_{s\beta}) \sigma_{LAG_{si}} R_{LAG_{si}} (r'_{si})^{-1} \end{aligned}$$

If both $Permit_{BV_i}^{\ell} = Permit_{BV_i}$ and $Left(4) = Right(4)$ hold, BV_{si} will regard LAG_s as a legal aggregator, and $\{BV_{si}, LAG_s\}$ will establish mutual authentication. StorageAP mainly considers BV_{si} 's user response related privacy preservation, in which LAG_s cannot obtain the real identity of the responsive BV_{si} , and cannot correlate BV_{si} 's response (e.g., *Agree*, or *Decline*) with its real identity.

D. S3PAP-C: Authentication Protocol for the S3P-BV in the Centralized Discharging Mode

Fig. 6 shows an interaction of $\{BV_{pci}, LAG_{pc}, CA\}$, and BV_{pci} represents a S3P-BV that agrees to participate in the discharging operation, and its stored power will be transmitted into the power grid for centralized energy dispatching.

1) *Phase 1. BV_{pci} Challenging LAG_{pc} :* BV_{pci} generates a session identifier $sid_{BV_{pci}}$, and transmits $sid_{BV_{pci}}$ to LAG_{pc} . Thereafter, LAG_{pc} also generates a session identifier $sid_{LAG_{pc}}$, and randomly chooses $\nu_{LAG_{pc}} \in \mathbb{Z}_q^*$ to compute $\{sid_{pci}, R_{LAG_{pc}}, S_{LAG_{pc}}, T_{LAG_{pc}}\}$. LAG_{pc} transmits the cascade message $sid_{LAG_{pc}} || R_{LAG_{pc}} || S_{LAG_{pc}} || T_{LAG_{pc}}$ to BV_{pci} for establishing a blind signature.

$$\begin{aligned} sid_{pci} &= H_0(sid_{BV_{pci}} || sid_{LAG_{pc}} || r_{si}^{\ell}) \\ R_{LAG_{pc}} &= (sid_{pci})^{x_{LAG}} \pmod{q} \\ S_{LAG_{pc}} &= g^{\nu_{LAG_{pc}}} \pmod{q} \\ T_{LAG_{pc}} &= (sid_{pci})^{\nu_{LAG_{pc}}} \pmod{q} \end{aligned}$$

2) *Phase 2. BV_{pci} Blinding Sensitive Message:* BV_{pci} randomly chooses $\{a_{BV_{pci}}, b_{BV_{pci}}\}$ from \mathbb{Z}_q^* , and extracts a message $m_{BV_{pci}}$, which may refer to BV_{pci} 's sensitive power value. BV_{pci} further re-computes sid_{pci}^{ℓ} , and obtains values $\{S_{BV_{pci}}, T_{BV_{pci}}\}$.

$$\begin{aligned} S_{BV_{pci}} &= (S_{LAG_{pc}})^{a_{BV_{pci}}} g^{b_{BV_{pci}}} \pmod{q} \\ T_{BV_{pci}} &= (T_{LAG_{pc}})^{a_{BV_{pci}}} (sid_{pci}^{\ell})^{b_{BV_{pci}}} \pmod{q} \end{aligned}$$

BV_{pci} computes the encrypted values $\{P_{BV_{pci}}, I_{BV_{pci}}\}$, and the hash related values $\{m_{BV_{pci}}, N_{BV_{pci}}\}$.

$$\begin{aligned} P_{BV_{pci}} &= E_{k_{BV_i}}(m_{BV_{pci}} || a_{BV_{pci}}) \\ I_{BV_{pci}} &= E_{k_{BV_i}}(PID_{BV_i} || b_{BV_{pci}}) \\ M_{BV_{pci}} &= H_0(S_{BV_{pci}} || T_{BV_{pci}} || P_{BV_{pci}} || I_{BV_{pci}}) \\ N_{BV_{pci}} &= M_{BV_{pci}} (a_{BV_{pci}})^{-1} \end{aligned}$$

Thereafter, BV_{pci} transmits the blinded message $N_{BV_{pci}}$ to LAG_{pc} for establishing a blind signature. Upon receiving the message, LAG_{pc} computes and replies $M_{LAG_{pc}}$ to BV_{pci} .

$$M_{LAG_{pc}} = \nu_{LAG_{pc}} + N_{BV_{pci}} \cdot x_{LAG} \pmod{q}$$

3) *Phase 3. BV_{pci} Verifying LAG_{pc} 's Blind Signature:* BV_{pci} computes $R_{BV_{pci}}$ to establish the signature with three-tuple $\{S_{BV_{pci}}, T_{BV_{pci}}, R_{BV_{pci}}\}$.

$$R_{BV_{pci}} = a_{BV_{pci}} M_{LAG_{pc}} + b_{BV_{pci}} \pmod{q}$$

BV_{pci} verifies LAG_{pc} by checking the following equations.

$$g^{R_{BV_{pci}}} \stackrel{?}{=} S_{BV_{pci}} (Y_{LAG})^{M_{BV_{pci}}} \quad (5)$$

$$(sid_{pci}^{\ell})^{R_{BV_{pci}}} \stackrel{?}{=} T_{BV_{pci}} (R_{LAG_{pc}})^{M_{BV_{pci}}} \quad (6)$$

- For the left side of (5), we have,

$$\begin{aligned} Left(5) &= g^{a_{BV_{pci}} M_{LAG_{pc}} + b_{BV_{pci}}} \\ &= g^{a_{BV_{pci}} \nu_{LAG_{pc}} + b_{BV_{pci}}} (Y_{LAG})^{a_{BV_{pci}} N_{BV_{pci}}} \end{aligned}$$

- For the right side of (5), we have,

$$\begin{aligned} Right(5) &= (S_{LAG_{pc}})^{a_{BV_{pci}}} g^{b_{BV_{pci}}} (Y_{LAG})^{M_{BV_{pci}}} \\ &= g^{\nu_{LAG_{pc}} a_{BV_{pci}} + b_{BV_{pci}}} (Y_{LAG})^{M_{BV_{pci}}} \end{aligned}$$

- For the left side of (6), we have,

$$\begin{aligned} Left(6) &= (sid_{pci}^{\ell})^{a_{BV_{pci}} M_{LAG_{pc}} + b_{BV_{pci}}} \\ &= (sid_{pci}^{\ell})^{a_{BV_{pci}} \nu_{LAG_{pc}} + M_{BV_{pci}} x_{LAG} + b_{BV_{pci}}} \end{aligned}$$

- For the right side of (6), we have,

$$\begin{aligned} Right(6) &= (T_{LAG_{pc}})^{a_{BV_{pci}}} (sid_{pci}^{\ell})^{b_{BV_{pci}}} \\ &= (sid_{pci}^{\ell})^{x_{LAG} M_{BV_{pci}}} \\ &= (sid_{pci}^{\ell})^{\nu_{LAG_{pc}} a_{BV_{pci}} + x_{LAG} M_{BV_{pci}}} \\ &= (sid_{pci}^{\ell})^{b_{BV_{pci}}} \end{aligned}$$

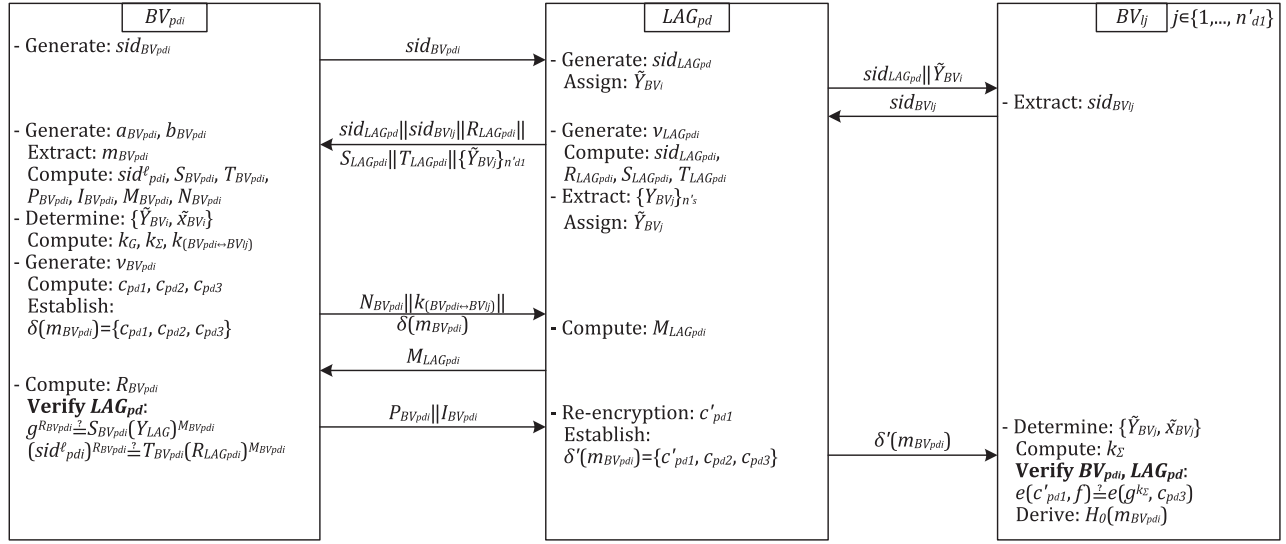


Fig. 7. S3PAP-D: The authentication protocol for the S3P-BV in the distributed discharging mode.

If $Left(5) = Right(5)$ and $Left(6) = Right(6)$ hold, BV_{pci} will regard LAG_{pc} as a legal aggregator, and transmit $P_{BV_{pci}} || I_{BV_{pci}}$ to LAG_{pc} . Thereafter, LAG_{pc} forwards $sid_{BV_{pci}} || sid_{LAG_{pc}} || P_{BV_{pci}} || I_{BV_{pci}}$ to CA for billing purposes. CA as a trusted entity, which can derive the detailed $m_{BV_{pci}}$ and $PID_{BV_{pci}}$ by decryption for both power tracing and identity tracing. The centralized discharging mode is launched based on the successful executions of LoadAP and StorageAP, and further focuses on the S3P-BV's power status privacy. When BV_{pci} performs the centralized discharging operation, the fair blind signature scheme ensures that BV_{pci} can ascertain LAG_{pc} 's validity without disclosing its sensitive energy status information.

E. S3PAP-D: Authentication Protocol in the Distributed Discharging Mode

Fig. 7. shows an interaction of $\{BV_{pdi}, LAG_{pd}, BV_{lj}\}$, and BV_{pdi} represents a S3P-BV to transmit its power to the neighboring load-BVs in the distributed discharging mode. BV_{lj} represents one of the neighboring load-BVs $\{BV_{l1}, \dots, BV_{ln'd1}\}$ ($j \in \{1, \dots, n'd1\}$, $n'd1 \in \mathbb{N}^*$) during the discharging operation. Here, $n'd1$ is the number of the BVs in BV_{lj} 's temporarily dynamic group. BV_{pdi} establishes communication with BV_{lj} via LAG_{pd} by the flexible energy support mode. During the distributed discharging mode, BV_{lj} may enjoy more convenient power services compared with the centralized mode, and also establishes active power status sharing with BV_{lj} , which brings an additional security challenge during communications.

1) *Phase 1. BV_{pdi} Challenging LAG_{pd} and BV_{plj} :* BV_{pdi} generates a session identifier $sid_{BV_{pdi}}$, and transmits $sid_{BV_{pdi}}$ to LAG_{pd} . Upon receiving the message, LAG_{pd} generates a session identifier $sid_{LAG_{pd}}$, and extracts the formerly received public keys $\{Y_{BV_i}\}_{n_s}$. LAG_{pd} assigns the i' -th element of $\{Y_{BV_i}\}_{n_s}$ as a pseudo public key $\tilde{Y}_{BV_i} = \{Y_{BV_i}\}_{i'=sid_{BV_{pdi}} \pmod{n_s}}$, and transmits $sid_{LAG_{pd}} || \tilde{Y}_{BV_i}$ to BV_{plj} for interconnection with BV_{plj} . BV_{plj} further extracts the formerly generated $sid_{BV_{plj}}$ as a response to LAG_{pd} .

Then, LAG_{pd} randomly chooses $v_{LAG_{pd}i} \in \mathbb{Z}_q^*$ to compute $\{sid_{pdi}, R_{LAG_{pd}i}, S_{LAG_{pd}i}, T_{LAG_{pd}i}\}$, in which $sid_{pdi} = H_0(sid_{BV_{pdi}} || sid_{LAG_{pd}} || sid_{BV_{plj}} || r_{si}^{\ell})$. LAG_{pd} also assigns the j' -th element of $\{Y_{BV_j}\}_{n'_s}$ as a pseudo public key $\tilde{Y}_{BV_j} = \{Y_{BV_j}\}_{j'=sid_{BV_{lj}} \pmod{n'_s}}$, in which n'_s refers to the number of BVs in BV_j 's affiliated static group. LAG_{pd} transmits $sid_{LAG_{pd}} || sid_{BV_{plj}}, R_{LAG_{pd}i} || S_{LAG_{pd}i} || T_{LAG_{pd}i}$, and $\{\tilde{Y}_{BV_j}\}_{n'_d1}$ to BV_{pdi} for blind signature generation. Note that $\{\tilde{Y}_{BV_j}\}_{n'_d1}$ refers to the public keys of other temporarily gathered load-BVs (i.e., $BV_{l1}, \dots, BV_{ln'd1}$).

2) *Phase 2. BV_{pdi} Blinding Sensitive Message, and Generating Group and Re-Encryption Keys:* The blind signature process is performed by the similar algorithms in S3PAP-C. It turns out that BV_{pdi} randomly chooses $\{a_{BV_{pdi}}, b_{BV_{pdi}}\} \in \mathbb{Z}_q^*$, extracts a power related message $m_{BV_{pdi}}$, and computes $\{S_{BV_{pdi}}, T_{BV_{pdi}}, P_{BV_{pdi}}, I_{BV_{pdi}}, M_{BV_{pdi}}, N_{BV_{pdi}}\}$ for establishing a blinded message. Afterwards, BV_{pdi} determines the pairwise pseudo keys $\{\tilde{Y}_{BV_i}, \tilde{x}_{BV_i}\}$, and computes two group keys $\{k_G, k_\Sigma\}$ based on $\{\tilde{Y}_{BV_1}, \dots, \tilde{Y}_{BV_{n'_d1}}\}$ and \tilde{Y}_{BV_j} respectively. Accordingly, a bidirectional re-encryption key $k_{(BV_{pdi} \leftrightarrow BV_{lj})}$ is established according to k_G and k_Σ .

$$k_G = \prod_{\gamma=1}^{n'_d1} (\tilde{Y}_{BV_\gamma})^{\tilde{x}_{BV_\gamma}} = g^{\tilde{x}_{BV_\gamma} \sum_{\gamma=1}^{n'_d1} \tilde{x}_{BV_\gamma}} \pmod{q}$$

$$k_\Sigma = (\tilde{Y}_{BV_j})^{\tilde{x}_{BV_j}} = g^{\tilde{x}_{BV_j} \tilde{x}_{BV_j}} \pmod{q}$$

$$k_{(BV_{pdi} \leftrightarrow BV_{lj})} = k_\Sigma / k_G$$

BV_{pdi} randomly generates $v_{BV_{pdi}} \in \mathbb{Z}_q^*$, and computes a set of values $\{c_{pd1}, c_{pd2}, c_{pd3}\}$, in which the parameters of the bilinear map has been defined in system initialization.

$$c_{pd1} = g^{k_G v_{BV_{pdi}}} \pmod{q}$$

$$c_{pd2} = e(g, H_1(PID_{LAG}))^{v_{BV_{pdi}}} H_0(m_{BV_{pdi}})$$

$$c_{pd3} = f^{v_{BV_{pdi}}} \pmod{q}$$

BV_{pdi} establishes the ciphertext $\delta(m_{BV_{pdi}})$ in the form of $\{c_{pd1}, c_{pd2}, c_{pd3}\}$, and transmits the blinded message $N_{BV_{pdi}}$

and $k_{(BV_{pdi} \leftrightarrow BV_{lji})} \|\delta(m_{BV_{pdi}})\|$ to LAG_{pd} . Then, LAG_{pd} computes and replies $M_{LAG_{pd}}$ to BV_{pdi} .

3) *Phase 3. BV_{pdi} Verifying LAG_{pd} 's Blind Signature, and LAG_{pd} Re-Encrypting BV_{pdi} 's Ciphertext:* BV_{pdi} computes $R_{BV_{pdi}}$ to establish a blind signature $R_{BV_{pdi}}$, and verifies LAG_{pd} by performing the similar algorithms in equations (5) and (6). If both equations hold, BV_{pdi} will transmit $P_{BV_{pdi}} \| I_{BV_{pdi}}$ to LAG_{pd} . Thereafter, LAG_{pd} performs re-encryption on c_{pd1} to obtain c'_{pd1} , and to establish a new ciphertext $\delta'(m_{BV_{pdi}}) = \{c'_{pd1}, c_{pd2}, c_{pd3}\}$.

$$c'_{pd1} = (c_{pd1})^{k_{(BV_{pdi} \leftrightarrow BV_{lji})}} = g^{g^{\tilde{x}_{BV_i} \tilde{x}_{BV_j} v_{BV_{pdi}}}} \pmod{q}$$

LAG_{pd} transmits $\delta'(m_{BV_{pdi}})$ to BV_{plj} for distributed power support. BV_{plj} first determines the pairwise pseudo keys $\{\tilde{Y}_{BV_j}, \tilde{x}_{BV_j}\}$ to compute $k_\Sigma = (\tilde{Y}_{BV_i})^{\tilde{x}_{BV_j}} = g^{\tilde{x}_{BV_i} \tilde{x}_{BV_j}}$ (mod q). BV_{plj} verifies $\{BV_{pdi}, LAG_{pd}\}$ by checking the following equation.

$$e(c'_{pd1}, f) \stackrel{?}{=} e(g^{k_\Sigma}, c_{pd3}) \quad (7)$$

- For the left side of (7), we have,

$$\begin{aligned} Left(7) &= e(g^{g^{\tilde{x}_{BV_i} \tilde{x}_{BV_j} v_{BV_{pdi}}}}, f) \\ &= e(g, f)^{g^{\tilde{x}_{BV_i} \tilde{x}_{BV_j} v_{BV_{pdi}}}} \end{aligned}$$

- For the right side of (7), we have,

$$\begin{aligned} Right(7) &= e(g^{(\tilde{Y}_{BV_i})^{\tilde{x}_{BV_j}}}, f^{v_{BV_{pdi}}}) \\ &= e(g^{g^{\tilde{x}_{BV_i} \tilde{x}_{BV_j}}}, f^{v_{BV_{pdi}}}) \end{aligned}$$

If $Left(7) = Right(7)$ holds, BV_{plj} will regard BV_{pdi} and LAG_{pd} as legal entities, and derive the hashed message $H_0(m_{BV_{pdi}})$ for establishing power interactions between BV_{pdi} and BV_{plj} . Afterwards, LAG_{pd} transmits $sid_{BV_{pdi}} \| sid_{LAG_{pd}} \| sid_{BV_{plj}}$ and $P_{BV_{pdi}} \| I_{BV_{pdi}}$ to CA for billing purposes.

$$\begin{aligned} H_0(m_{BV_{pdi}}) &= c_{pd2} e(c'_{pd1}, H_1(PID_{LAG}))^{-1/k_\Sigma} \\ &= e(g, H_1(PID_{LAG}))^{v_{BV_{pdi}}} H_0(m_{BV_{pdi}}) \\ &= e(g^{g^{\tilde{x}_{BV_i} \tilde{x}_{BV_j} v_{BV_{pdi}}}}, H_1(PID_{LAG}))^{-1/(\tilde{Y}_{BV_i})^{\tilde{x}_{BV_j}}} \end{aligned}$$

In S3PAP-D, BV_{pdi} has successfully performed LoadAP and StorageAP, and BV_{lji} also has executed LoadAP to establish mutual authentication with its corresponding local aggregator. S3PAP-D mainly focuses on the energy status privacy, and LAG_{pd} can only determine BV_{pdi} and BV_{lji} 's group attribute by introducing the set of public keys in its static group, and BV_{plj} can only obtain BV_{lji} 's hashed power value $H_0(m_{BV_{pdi}})$ for determining its share of power. In particular, BV_{pdi} 's total discharging status cannot be exposed to LAG_{pd} or BV_{lji} , and BV_{lji} 's individual charging status cannot be correlated with its specific identity by LAG_{pd} or BV_{pdi} .

V. SUB-PROTOCOLS INTER-RELATIONSHIP DISCUSSION

In ROPS, the proposed sub-protocols (i.e., LoadAP, StorageAP, and S3PAP-C/S3PAP-D) are interlinked with each other. We will discuss the scheme inter-relationships based on the associated cryptographic primitives.

- 1) *Session Identifier:* Session identifiers are generated by the involved entities, and are reused through the whole scheme. In LoadAP, $\{BV_{li}, LAG_l\}$ respectively generate $\{sid_{BV_{li}}, sid_{LAG_l}\}$, which are applied to declare their group attributes, and to obtain the combined session identifier sid_{li} . The re-computed sid_{li}^{ℓ} is also introduced for normalization to achieve BV_{li} verifying LAG_l 's signature. In StorageAP, $\{sid_{li}, sid_{LAG_{li}}\}$ are introduced to obtain the random numbers $\{r_{si}, r_{LAG_{si}}\}$. In S3PAP-C, $\{sid_{BV_{pei}}, sid_{LAG_{pe}}\}$ are applied to re-structure sid_{pei} for establishing a blind signature, and $\{sid_{BV_{pdi}}, sid_{LAG_{pd}}, sid_{BV_{lji}}\}$ are similarly introduced to obtain sid_{pdi} in S3PAP-D. Such progressive session identifiers correlate the sub-protocols, and previous illegal interactions may not influence the ongoing and subsequent communications.
- 2) *Pseudorandom number:* In StorageAP, r_{CA} is generated to obtain $r_{LAG_{si}}$ by computing $H_0(sid_{LAG_{li}} \oplus r_{CA})$, and $\{r_{LAG_{si}}, r_{CA}\}$ are applied to wrap the pseudonyms $\{PID_{BV_i}, PID_{LAG}\}$ for CA 's verification. The re-structured pseudorandom number r_{si} involving $\{r_{BV_{si}}, r_{LAG_{si}}, sid_{li}\}$ is applied to link StorageAP and S3PAP, and is also used to obtain the normalized elements $\{r'_{s1}, \dots, r'_{sn_{d2}}\}$. Meanwhile, r_{si} is further applied to obtain sid_{pei}/sid_{pdi} in S3PAP-C/S3PAP-D for establishing blind signatures.
- 3) *Static group and dynamic group:* BVs can be organized in a static group and a dynamic group. Thereinto, n_s/n'_s is used to represent the number of BVs in a BV's static group that is assigned by a specific power operator. $\{n_{d*}\}$ (i.e. n_{d1}/n'_{d1} , and n_{d2}) indicates the number of a BV's dynamic group that is established by the temporarily gathered BVs around the same LAG 's range. n_s is used by BV_i to establish the ring signatures in LoadAP and StorageAP, and to assign the pairwise pseudo keys for during group key agreement in S3PAP-D. $\{n_{d*}\}$ varies according to dynamic interactions, and is applied by LAG to determine the number of transmitted messages through the ROPS.

VI. SECURITY ANALYSIS

A. Privacy Preservation

Privacy preservation mainly revolves around the individual identity to provide a pseudonymous identification and authentication mechanism. In the ROPS, the interlinked sub-protocols exploit ring signature or fair blind signature algorithms to achieve enhanced privacy preservation, which guarantees that LAG cannot correlate BV_i 's real identity with its sensitive information (e.g., location, user response, and energy status).

- In LoadAP, BV_{li} establishes a ring signature on behalf of other BVs in its static group, therefore LAG_l can only ascertain BV_{li} 's general group attribute. The pseudonym

PID_{BV_i} is wrapped by the individual key k_{BV_i} , which is only shared by BV_i and CA . Such anonymous data transmission realizes that LAG_l cannot derive BV_{li} 's pseudonym, and LAG_l can only guess BV_{li} 's real identity with the probability $1/n_s$. Meanwhile, LAG_l generates an operator for the temporarily gathered BVs, and addresses the BVs as a dynamic group. The ciphertext $M_{BV_{li}}$ is transmitted to CA for further identification. Thus, LAG_l and other adversaries cannot correlate BV_{li} 's real identity with its location information.

- In StorageAP, BV_{si} computes an irreversible hash value $M_{BV_{si}}$ to hide PID_{BV_i} , in which a random operator $r_{LAG_{si}}$ is introduced to enhance data randomness. Similarly, BV_{si} also establishes a ring signature to conceal its real identity, and LAG_s cannot determine if the received nonspecific response $m_{BV_{si}}$ (i.e., *Agree*, or *Decline*) comes from BV_{si} . Thus, LAG_s cannot estimate BV_{si} 's user response information.
- In S3PAP-C, BV_{pci} adopts a fair blind signature including $\{S_{BV_{pci}}, T_{BV_{pci}}, R_{BV_{pci}}\}$ to hide the sensitive message $m_{BV_{pci}}$. Meanwhile, $\{m_{BV_{pci}}, PID_{BV_i}\}$ are respectively encrypted into $\{P_{BV_{pci}}, I_{BV_{pci}}\}$ for anonymous transmission. Such authentication scheme achieves that LAG_{pc} can obtain BV_{pci} 's neither power information nor identity information, and also cannot correlate BV_{pci} 's energy status with its real identity.
- In S3PAP-D, an enhanced authentication is applied compared with S3PAP-C to achieve private power interactions between BV_{pdi} and $\{BV_{lj}\}_{n'_{d1}}$ (i.e., $\{BV_{l1}, \dots, BV_{ln'_{d1}}\}$). When BV_{pdi} directly feeds its own energy to the multiple neighboring load-BVs $\{BV_{lj}\}_{n'_{d1}}$, BV_{pdi} 's total discharging status is protected by $H_0(m_{BV_{pdi}})$, and BV_{lj} can only determine its own share of power. The pseudo public keys $\{\tilde{Y}_{BV_i}, \tilde{Y}_{BV_j}\}$ are assigned according to the i' -th or j' -th public key in BV_{pdi} or BV_{lj} 's static group, in which $i' = sid_{BV_{pdi}} \pmod{n_s}$ and $j' = sid_{BV_{lj}} \pmod{n'_s}$. Two group keys k_G and k_Σ are respectively obtained by involving $\{\tilde{Y}_{BV_1}, \dots, \tilde{Y}_{BV_{n'_{d1}}}\}$ and \tilde{Y}_{BV_j} . Furthermore, a re-encryption key $k_{(BV_{pdi} \leftrightarrow BV_{lj})}$ is established based on $\{k_G, k_\Sigma\}$, and is used by LAG_{pdi} to re-encrypt c_{pdi} into c'_{pdi} . Upon receiving the re-encrypted ciphertext, BV_{lj} performs decryption by its own pseudo privacy key \tilde{x}_{BV_j} without revealing any BV_{pdi} 's sensitive keys.

B. Session Freshness

Session identifiers and pseudorandom numbers are jointly applied to achieve session freshness and unlinkability. Thereinto, $\{sid_{BV_{li,pci/pdi}}, sid_{LAG_l,pc/pd}\}$ are respectively generated by $\{BV_i, LAG\}$. Such session identifiers are re-structured into $sid_{li,pci/pdi}$ by the hash function $H_0(\cdot)$, in which sid_{li} is applied to wrap $E_{LAG_{li}}$ for CA 's identification, and $sid_{pci/pdi}$ is used as a random operator in the blind signature. Moreover, sid_{LAG_l} is extended into $\{sid_{LAG_{li}}\}_{n_{d1}}$ by extension operation, and $sid_{LAG_{li}}$ is further used to obtain $r_{LAG_{li}}$ in StorageAP. Towards pseudorandom numbers, r_{CA} is generated to obtain $r_{LAG_{si}}$, which is jointly applied along with $r_{BV_{si}}$ to compute r_{si} in StorageAP. Besides, two re-computed session-variables

$\{sid_{li}^\ell, r_{si}^\ell\}$ are normalized into $\{sid'_{li}\}_{n_{d1}}$ and $\{r'_{si}\}_{n_{d2}}$ for BV_i 's verification on LAG .

C. Hierarchical Access Control

Hierarchical access control provides diverse authorities on an entity's secret key and pseudonym towards different authentication entities such that sensitive data can only be derived by a certain authorized entity. In ROPS, $\{LAG, CA\}$ have different authorities on BV_i , while $\{LAG, BV_i\}$ have dissimilar authorities on each other. Such hierarchical access control is achieved by the ring signature and pseudonym based asymmetrical authority and authority separation mechanisms.

- For LAG : LAG can only obtain BV_i 's general group attribute (including the number of the static and dynamic in-group BVs) according to the ring signatures without revealing its real identity. During ring signature and group/re-computed key agreement, LAG can only obtain a set of public keys owned by all the BVs in BV_i 's static group, without exposing an individual public key for identification. Meanwhile, LAG cannot derive BV_i 's wrapped pseudonym PID_{BV_i} to determine BV_i 's individual identity.
- For CA : CA can derive BV_i 's pseudonym PID_{BV_i} by the secret key k_{BV_i} based decryption, and further determine BV_i 's real identity for billing purposes. CA can also derive $\{m_{BV_{pci}}, PID_{BV_i}\}$ from $P_{BV_{pci}}$ and $I_{BV_{pci}}$ for both power tracing and identify tracing, which improves the limitation of the traditional blind signature.
- For BV_i : BV_i owns LAG 's pseudonym PID_{LAG} , and its public keys Y_{LAG}/Y'_{LAG} to confirm which LAG it is communicating with. Accordingly, BV_i verifies LAG 's validity by the pre-assigned cryptographic operators.

D. Data Confidentiality and Data Integrity

Data confidentiality is achieved by encryptions, in which the one-session available key k_{BV_i} shared by BV_i and CA , and $\{k_G, k_\Sigma\}$ are dynamically established between a distributed discharging S3P-BV and neighboring load-BVs. In LoadAP, k_{BV_i} is applied to hide BV_{li} 's pseudonym PID_{BV_i} into $M_{BV_{li}}$, which is not exposed and can only be decrypted by CA . In S3PAP, $\{P_{BV_{pi}}, I_{BV_{pi}}\}$ ($p \in \{pc, pd\}$) are also computed based on k_{BV_i} for sensitive message hiding. Particularly, a group key k_Σ is applied to encrypt k_G for transmission, and a bidirectional key $k_{(BV_{pdi} \leftrightarrow BV_{lj})}$ is used for re-encryption in S3PAP-D. Data integrity is accomplished by applying one-way hash functions. In ROPS, $H_0(\cdot)$ is applied to obtain $\{sid_{*i}, r_{*i}\}$. Particularly, $\{PID_{BV_i}, PID_{LAG}\}$ are hashed into the forms of $\{M_{BV_{si}}, M_{LAG_s}\}$ in StorageAP, and hence attackers cannot modify the transmitted data. Additionally, the hash functions $\{H_1(\cdot), H_2(\cdot)\}$ are used in the signature algorithms to ensure the integrity of the challenged messages $\{m_{BV_{si}}, m_{LAG_{si}}\}$.

Additionally, mutual authentication is performed to achieve the trust relationship between BV_i and LAG in LoadAP and StorageAP, in which BV_i establishes the ring signatures $\{\delta(m_{BV_{li}}), \delta(m_{BV_{si}})\}$ for declaring its static group identity to LAG . LAG also establishes signatures that are used by

BV_i for authentication. Here, $\{BV_i, LAG\}$ verify each other according to the defined relationships between the pairwise public key and the private key. Meanwhile, the pseudonyms $\{PID_{BV_i}, PID_{LAG}\}$ are also adopted by CA to authenticate BV_i and LAG in StorageAP. Based on the mutual authentication in the first two sub-protocols, S3PAP-C/S3PAP-D mainly focuses on $BV_{p_c, p_{di}}$ and l or BV_{ij} sensitive power status, and provides unilateral authentication on LAG .

VII. CONCLUSION

In this paper, we first observed that a BV may act as an energy customer, storage or generator in V2G networks, and further identified dissimilar security challenges according to a BV's different roles. Then, we proposed a role-dependent privacy preservation scheme (ROPS) with anonymous authentication. The proposed scheme includes a set of sub-protocols (i.e., LoadAP, StorageAP, S3PAP-C, and S3PAP-D). We outlined both centralized and distributed discharging operations when a BV serves as an energy generator. The two operations provide very flexible energy supply to either the central smart grid or the local neighboring charging BVs. Security analysis indicates that ROPS satisfies security properties with respect to privacy preservation, session freshness, hierarchical access control, and data confidentiality and integrity. The identified new secure challenge and the proposed ROPS demonstrate the importance of role-awareness for securing V2G networks.

REFERENCES

- [1] H. Gharavi and R. Ghafurian, "Smart grid: The electric energy system of the future," *Proc. IEEE*, vol. 99, no. 6, pp. 917–921, Jun. 2011.
- [2] Y. Zhang, R. Yu, M. Nekovee, Y. Liu, S. Xie, and S. Gjessing, "Cognitive machine-to-machine communications: Visions and potentials for the smart grid," *IEEE Netw. Mag.*, vol. 26, no. 3, pp. 6–13, Jun. 2012.
- [3] M. Yilmaz and P. T. Krein, "Review of the impact of vehicle-to-grid technologies on distribution systems and utility interfaces," *IEEE Trans. Power Electron.*, vol. 28, no. 12, pp. 5673–5689, Dec. 2013.
- [4] C. Liu, K. T. Chau, D. Wu, and S. Gao, "Opportunities and challenges of vehicle-to-home, vehicle-to-vehicle, and vehicle-to-grid technologies," *Proc. IEEE*, vol. 101, no. 11, pp. 2409–2427, Nov. 2013.
- [5] A. Y. Saber and G. K. Venayagamoorthy, "Efficient utilization of renewable energy sources by gridable vehicles in cyber-physical energy systems," *IEEE Syst. J.*, vol. 4, no. 3, pp. 285–294, Sep. 2010.
- [6] A. Y. Saber and G. K. Venayagamoorthy, "Intelligent unit commitment with vehicle-to-grid—A cost-emission optimization," *J. Power Sour.*, vol. 195, no. 3, pp. 898–911, Feb. 2010.
- [7] 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 Trans. Smart Grid*, vol. 2, no. 4, pp. 697–706, Dec. 2011.
- [8] H. Guo, Y. Wu, F. Bao, H. Chen, and M. Ma, "UBAPV2G: A unique batch authentication protocol for vehicle-to-grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 707–714, Dec. 2011.
- [9] H. Liu, H. Ning, Y. Zhang, and L. T. Yang, "Aggregated-proofs based privacy-preserving authentication for V2G networks in the smart grid," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1722–1733, Dec. 2012.
- [10] H. Liu, H. Ning, Y. Zhang, and M. Guizani, "Battery status-aware authentication scheme for V2G networks in smart grid," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 99–110, Mar. 2013.
- [11] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Security mechanism for multi-domain vehicle-to-grid infrastructure," in *Proc. IEEE Global Telecommun. Conf.*, Dec. 2011, pp. 1–5.
- [12] H. Tseng, "A secure and privacy-preserving communication protocol for V2G networks," in *Proc. IEEE WCNC*, Apr. 2012, pp. 2706–2711.
- [13] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: Cyber attacks, countermeasures, and challenges," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 38–45, Aug. 2012.
- [14] M. Qiu, H. Su, M. Chen, Z. Ming, and L. T. Yang, "Balance of security strength and energy for a PMU monitoring system in smart grid," *IEEE Commun. Mag.*, vol. 50, no. 5, pp. 142–149, May 2012.
- [15] D. He, C. Chen, S. Chan, Y. Zhang, J. Bu, and M. Guizani, "Secure service provision in smart grid communications," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 53–61, Aug. 2012.
- [16] Z. M. Fadlullah, N. Kato, R. Lu, X. Sheng, and Y. Nozaki, "Toward secure targeted broadcast in smart grid," *IEEE Commun. Mag.*, vol. 50, no. 5, pp. 150–156, May 2012.
- [17] X. Wang and P. Yi, "Security framework for wireless communications in smart distribution grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 809–818, Dec. 2011.
- [18] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.
- [19] S. Kim, E. Lee, D. Je, and S. Seo, "A physical and logical security framework for multilevel AFCI systems in smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 3, pp. 496–506, Sep. 2011.
- [20] Q. Li and G. Cao, "Multicast authentication in the smart grid with one-time signature," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 686–696, Dec. 2011.
- [21] H. Son, T. Y. Kang, H. Kim, and J. H. Roh, "A secure framework for protecting customer collaboration in intelligent power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 759–769, Dec. 2011.
- [22] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, Dec. 2011.
- [23] Y. Kim, V. Kolesnikov, H. Kim, and M. Thottan, "SSTP: A scalable and secure transport protocol for smart grid data collection," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Oct. 2011, pp. 161–166.
- [24] M. Qiu, W. Gao, M. Chen, J. W. Niu, and L. Zhang, "Energy efficient security algorithm for power grid wide area monitoring system," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 715–723, Dec. 2011.
- [25] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 375–381, Jun. 2011.
- [26] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 238–243.
- [27] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621–1631, Sep. 2012.
- [28] X. Lin, R. Lu, H. Zhu, P. H. Ho, X. Shen, and Z. Cao, "ASRPAKE: An anonymous secure routing protocol with authenticated key exchange for wireless ad hoc networks," in *Proc. IEEE ICC*, Jun. 2007, pp. 1247–1253.
- [29] M. Stadler, J. Piveteau, and J. Camenisch, "Fair blind signatures," in *Proc. EUROCRYPT*, vol. 921, May 1995, pp. 209–219.
- [30] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in *Proc. 5th Int. Conf. ACNS*, Jun. 2007, pp. 288–306.



Hong Liu is currently working toward the Ph.D. degree at the School of Electronic and Information Engineering, Beihang University, China. She focuses on the security and privacy issues in radio frequency identification, vehicle-to-grid, and wireless machine-to-machine networks. Her research interests include authentication protocol design, and security formal modeling and analysis.



Huansheng Ning received the B.S. degree from Anhui University in 1996 and Ph.D. degree from Beihang University in 2001. He is a professor in the School of Computer and Communication Engineering, University of Science and Technology Beijing, China. His current research focuses on Internet of Things, aviation security, electromagnetic sensing and computing. He has published more than 50 papers in journals, international conferences/workshops.



Yan Zhang received a Ph.D. degree from Nanyang Technological University, Singapore. Since August 2006, he has been working with Simula Research Laboratory, Norway. He is currently senior research scientist at Simula Research Laboratory, Norway. He is an adjunct Associate Professor at the University of Oslo, Norway. He is a regional editor, associate editor, on the editorial board, or guest editor of a number of international journals. His research interests include wireless networks and smart grid communications.



Laurence T. Yang received his B.E. degree in computer science from Tsinghua University, China, and his Ph.D. degree in computer science from the University of Victoria, Canada. He is a professor in the School of Computer Science and Technology at Huazhong University of Science and Technology, China, and in the Department of Computer Science, St. Francis Xavier University, Canada. His research interests include parallel and distributed computing, and embedded and ubiquitous/pervasive computing. His research is supported by the National Sciences and Engineering Research Council and the Canada Foundation for Innovation.



satellite communication.

Qingxu Xiong received the Ph.D. degree in electrical engineering from Peking University, Beijing, China, in 1994. From 1994 to 1997, he worked in the Information Engineering Department at Beijing University of Posts and Telecommunications as a Postdoctoral Researcher. He is currently a Professor in the School of Electrical and Information Engineering at Beijing University of Aeronautics and Astronautics, Beijing, China. His research interests include scheduling in optical and wireless networks, performance modeling of wireless networks, and