A Privacy-Preserving Scheme for Incentive-Based Demand Response in the Smart Grid

Yanmin Gong, *Student Member, IEEE*, Ying Cai, *Member, IEEE*, Yuanxiong Guo, *Member, IEEE*, and Yuguang Fang, *Fellow, IEEE*

***Abstract*—The advanced metering infrastructure (AMI) in the smart grid provides real-time information to both grid operators and customers, exploiting the full potential of demand response (DR). However, it introduces new privacy threats to customers. Prior works have proposed privacy-preserving methods in the AMI, such as temporal or spatial aggregation. A main assumption in these works is that fine-grained data do not need to be attributable to individuals. However, this assumption does not hold in incentive-based demand response (IDR) programs where fine-grained metering data are required to analyze individual demand curtailments, and hence, need to be attributable. In this paper, we propose a privacy-preserving scheme for IDR programs in the smart grid, which enables the DR provider to compute individual demand curtailments and DR rewards while preserving customer privacy. Moreover, a customer can reveal his/her identity and prove ownership of his/her power usage profile in certain situations, such as legal disputes. We achieve both privacy and efficiency in our scheme through a combination of several cryptographic primitives, such as identity-committable signatures and partially blind signatures. As far as we know, we are the first to identify and address privacy issues for IDR programs in the smart grid.**

***Index Terms*—Billing, customer baseline (CBL), data privacy, demand response (DR), smart grid.**

I. Introduction

THE SMART grid is a modernized power grid that uses the information and communication technologies to improve the efficiency, reliability, economics, and sustainability of the generation, transmission, distribution, and consumption of electricity. In the smart grid, a full measurement and collection system called the advanced metering infrastructure (AMI) replaces traditional electromechanical meters. The AMI collects fine-grained, time-based information and transmits them to various parties through a communication network, enabling the integration of demand-side resources into the wholesale market and hence the demand response (DR).

According to the U.S. Department of Energy, DR refers to “changes in electric use by demand-side resources from their normal consumption patterns in response to the varying electricity price, or to incentive payments designed to reduce electricity use when wholesale market prices are high or when system reliability is jeopardized” [1]. In the power grid, generation and consumption should be balanced instantaneously. The load-following strategy, where a power plant adjusts its power supply to match the fluctuating demand, has been dominant in the traditional power grid operations. However, this strategy incurs a high cost in terms of environment, grid reliability, and operational efficiency. On the contrary, the smart grid places great emphasis on the DR strategy where consumers shape their power demand to match the supply [2]. DR supports high penetration of renewable energy generation by shaping the demand to match the intermittent and unpredictable power output of renewable generation, and it also brings other benefits such as peak shaving, reliability enhancement, and generation cost reduction.

Generally speaking, there are two types of DR programs: 1) price-based demand response (PDR) programs that motivate customers to change their consumption patterns according to time-varying electricity prices; and 2) incentive-based demand response (IDR) programs that reward participating customers for reducing their electricity usage in response to DR requests. Although more utilities offer some types of PDR programs to customers than IDR programs, PDR accounts for just a small part of the total DR resource base [3]. Since IDR programs can be tailored to specific operational goals such as localized load reduction during transmission congestion, they diversify the ways in which demand-side management contributes to reliable and efficient grid operations. In IDR programs, the time interval of measurements varies from hours to seconds based on different trigger conditions [4], which poses a serious threat to customer privacy [5], [6]. It has been shown that power usage profiles at a granularity of 15 min may reveal whether a child is left alone at home and at a finer granularity may reveal the daily routines of customers [7]. Despite its importance, the privacy issues in IDR programs have never been addressed before. The unique challenge of IDR programs lies in the fact that the meter measurements

Manuscript received October 14, 2014; revised January 25, 2015; accepted February 2, 2015. Date of publication March 25, 2015; date of current version April 19, 2016. This work was supported by the U.S. National Science Foundation under Grant CNS-1343356 and Grant CNS-1423165. The work of Y. Cai was supported in part by the Opening Project of the Beijing Key Laboratory of Internet Culture and Digital Dissemination Research under Grant ICDD-201408. Paper no. TSG-01018-2014.

Y. Gong and Y. Fang are with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611 USA (e-mail: fang@ece.ufl.edu).

Y. Cai is with the Department of Computer Science and Technology, Beijing Information Science and Technology University, Beijing 100101, China, and also with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China.

Y. Guo is with the School of Electrical and Computer Engineering, Oklahoma State University, Stillwater, OK 74078 USA.

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/TSG.2015.2412091

should be both attributable and fine-grained, excluding some popular privacy-preserving approaches that address privacy issues in PDR programs. In IDR programs, there is a new party called the demand response provider (DRP), who aggregates demand-side resources of customers and rewards customers based on their demand curtailments in DR events. The DRP can either be the electric utility company or a third party, and it collects fine-grained metering measurements in order to calculate the customer baseline (CBL) and hence the demand curtailments.

In this paper, we aim at preserving customer privacy for IDR programs in the smart grid. We propose a scheme that enables the DRP to profile, reward, and provide feedback to customers in IDR programs without violating customer privacy. The DRP is able to analyze fine-grained metering data to calculate CBLs, schedule demand curtailments, and correctly reward customers, but it cannot link the real identity of a customer to the fine-grained metering data. Our scheme is constructed by cryptographic primitives. Individual metering data are signed with a special technique such that the authenticity can be verified without revealing the real identity of the signer. When customers want to inquire their metering data or claim their DR rewards, they prove their eligibility to the DRP but reveal no additional information about themselves. With these techniques combined, the anonymity of customers is guaranteed throughout the IDR processes. As far as we know, we are the first to address the privacy issues in IDR programs.

The rest of this paper is organized as follows. Section II presents the cryptographic primitives used in our scheme. We provide some background on IDR programs and describe the components, system flow, and design goals of our scheme in Section III. Section IV elaborates on the proposed scheme, where we design privacy-preserving protocols for different processes in IDR programs. Practical considerations and useful extensions are presented in Section V. Sections VI and VII analyze the security and the efficiency of the proposed scheme, respectively. Related work is provided in Section VIII. Finally, Section IX concludes this paper.

II. Cryptographic Primitives

This section gives an introduction to the cryptographic primitives used as the building blocks in our scheme.

A. Identity-Committable Signature

The identity-based signature scheme [8] avoids the use of certificates in conventional public key infrastructure by deriving the public key of a signer from his public identity information such as e-mail address and telephone number. The scheme designed in [9] makes use of a bilinear pairings on elliptic curves, a popular technique in identity-based public key cryptography. Let $\mathbb{G}$ be an additive group with generator P and $\mathbb{G}_T$ be a multiplicative group. A mapping $\hat{e} : \mathbb{G} \times \mathbb{G} = \mathbb{G}_T$ is called a bilinear pairing if it satisfies the following.

1) *Bilinearity:* $\hat{e}(aP, bP) = \hat{e}(P, Q)^{ab}$ for all $a, b \in Z_p$ and $P \in \mathbb{G}$.
2) *Nondegeneracy:* If P is a generator of G, then $\hat{e}(P, P) \neq 1$.
3) *Computability:* There exists an efficient algorithm to compute $\hat{e} = (P, Q)$ for all $P, Q \in \mathbb{G}$.

Based on the identity-based signature scheme, Chu and Tzeng [10] constructed an identity-committable signature (ICS) scheme which allows a signer to sign a message on behalf of an organization or a group.

The scheme is setup as follows. The private key generator (PKG) chooses a master secret key $(x, y) : x, y \in_R \mathbb{Z}_p$ and three hash functions $H_1 : \{0, 1\}^* \to \mathbb{G}, H_2 : \{0, 1\}^* \times \mathbb{G} \to \mathbb{Z}_p$, and $H_2' : \{0, 1\}^* \times \mathbb{G} \times \mathbb{G} \to \mathbb{Z}_p$. Then it computes $P_X = xP$, $P_Y = yP$ and publishes $(\mathbb{G}, \mathbb{G}_T, \hat{e}, P, P_X, P_Y, H_1, H_2, H_2')$ as the public parameters. For identity I, the DRP calculates $Q_I = H_1(I)$, $Q_I' = xQ_I$, and $S_I = xyQ_I$. The public and private key pairs for the user are Q_I and (Q_I', S_I), respectively. To generate an ICS on message m, the signer randomly selects a value $r \in Z_p$, computes $h = H_2(m, U)$, and generates $U_I = rQ_I'$, $V_I = (r + h)S_I$. The signer then chooses a secret $\mu \in Z_p^* \setminus \{1\}$ and computes $Q = \mu Q_I$, $Q' = \mu Q_I'$, $U = \mu U_I$, and $V = \mu V_I$. The ICS on message m is $\delta_{\mathrm{IC}} = (Q, Q', U, V)$. To verify the signature, the verifier calculates $h = H_2'(m, Q, U)$ and accepts the signature if and only if $\hat{e}(Q, P_X) = \hat{e}(Q', P)$ and $\hat{e}(U, P_Y) = \hat{e}(V, P)\hat{e}(Q', -P_Y)^h$ hold.

B. Zero-Knowledge Proof

The notion of zero-knowledge proof (ZKP) is introduced by Goldwasser *et al.* [11], in which the prover takes interactive input from the verifier and responds based on this input. With the Fiat-Shamir [12] heuristic, the ZKP can be transformed into the noninteractive form where interaction is not needed between the verifier and the prover. We follow the notions introduced by Camenisch and Stadler [13] to describe the ZKP protocols and let PK$\{\cdot\}$ denotes the ZKP of a statement. For instance, PK$\{\alpha : C = g^\alpha\}$ is used to prove the knowledge of the discrete logarithm of C with base g. This is equivalent to the knowledge of α that satisfies the expression on the right side of the colon.

C. Partially Blind Signature

Commitment schemes enable one to commit a chosen value without revealing it. A well-known commitment scheme is the Pedersen commitment [14]. Let $\mathbb{G}$ be a group of prime order p and g and h be generators of $\mathbb{G}$. To commit a value $x \in \mathbb{Z}_p$, the committer randomly chooses $r \in \mathbb{Z}_p$, computes $C = g^x h^r$, and outputs C as the commitment. To reveal x, the committer discloses x, r. The verifier can verify if $C = g^x h^r$. Multiple values can be committed in a single commitment. For example, the commitment for x_1, x_2 is $C = g_1^{x_1} g_2^{x_2} h^r$, where g_1, g_2 are generators of $\mathbb{G}$. We denote the Pedersen commitment on message x as CM(x).

An application of commitment schemes is the BBS+ signature designed in [15] and [16]. The construction of BBS+ signature is partially blinded: the signer can sign messages in a commitment without knowing their values. Let $\mathbb{G}$, $\mathbb{G}_T$ be two cyclic groups of prime order p and $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ be a bilinear pairing function. Let $g, g_0, g_1, g_2 \in \mathbb{G}$ be generators of $\mathbb{G}$, which are public parameters. The signer randomly chooses $\gamma \in \mathbb{Z}_p$ as his secret key and computes $\omega = g^\gamma$ as

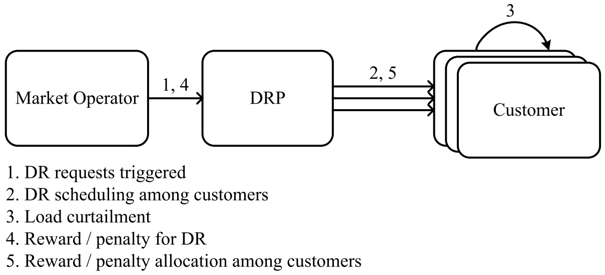

3
Market Operator
1, 4
DRP
2, 5
Customer
1. DR requests triggered
2. DR scheduling among customers
3. Load curtailment
4. Reward / penalty for DR
5. Reward / penalty allocation among customers

Fig. 1. Electricity market for IDR.

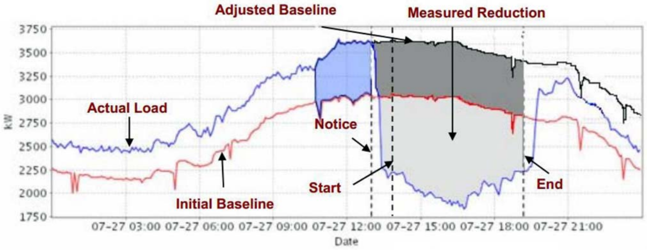


Fig. 2. Example baseline and performance measurement for DR asset [4].

his public key. To sign messages m_1, m_2, the signer randomly chooses $c, z \in Z_p$, computes $A = (gg_0^z g_1^{m_1} g_2^{m_2})^{1/(c+\gamma)}$, and outputs (A, c, z) as the signature. One can verify a BBS+ signature by checking if $\hat{e}(A, \omega g^c) = \hat{e}(gg_0^z g_1^{m_1} g_2^{m_2}, g)$ holds.

III. System Model

We describe the system model of the proposed privacy-preserving scheme in this section.

A. Background

As shown in Fig. 1, the electricity market for IDR involves three entities: 1) the market operator; 2) the DRP; and 3) the customers. The market operator manages the electricity market and triggers DR events based on the status of the power grid. When a DR event is triggered, the DRP schedules load curtailment among customers and aggregates these demand-side resources. Participating customers reduce their load during a DR event as scheduled. The market operator pays the DRP for its aggregate curtailment, and the DRP then allocates the reward among participating customers. Since customers have unequal contributions to the aggregate load curtailment, they should be rewarded based on their contributions so that active customers are encouraged.

Individual customer contribution is calculated as the difference between his real-time power consumption and his CBL, which represents the "behave-as-usual" usage pattern of a customer. Calculation of CBL is among the most important factors in an IDR program because it should neither reward nor penalize a customer for his natural load variances. Fig. 2 (depicted by [4]) gives an example of CBL, where the initial baseline is adjusted according to the actual load on that day so that the effort of demand reduction of the customer can be fairly estimated. In order to estimate the "behave-as-usual" usage pattern for a specific day, the input of the CBL calculation algorithm is an extensive data set including both fine-grained historical meter measurements and peripheral data (e.g., weather and time of the day) [4], [17]. However, these fine-grained metering data as required by the DRP in the CBL and curtailment calculation raise serious customer privacy concerns.

B. Components

To address these privacy concerns, we propose a scheme which enables the DRP to perform all the required operations without linking customer identity and fine-grained metering data. The scheme involves four components: 1) smart meters; 2) proxy; 3) DRP; and 4) customer devices.

1) Smart Meters: The utility company installs smart meters at customer premises, one for each customer. Smart meters are assumed to be tamper-resistant and able to perform elementary cryptographic operations, but they cannot store long-term metering data or perform CBL calculation due to limited storage and computation capabilities.

2) Proxy: The proxy plays the role of an anonymizer which hides the static IP address of smart meters. It can be either the gateway or a trusted third party. The proxy is semi-trusted, meaning curious but not malicious, in the sense that it may attempt to learn the customer privacy, but it will faithfully relay the metering data and hide the smart meter IP address from the DRP. From now on, when we refer to "anonymous channel," we mean an anonymous communication channel established by the proxy.

3) DRP: The DRP schedules DR events among customers, records customer performance in DR events, and calculates their corresponding rewards. The DRP is semi-trusted, meaning that it may attempt to learn the customer privacy, but it will faithfully follow protocol specifications.

4) Customer Devices: Customers query the DRP to learn their own metering data and claim DR rewards through customer devices (e.g., personal computers or smartphones). Customers are assumed to be curious and potentially malicious. They may impersonate other customers or collude with the DRP to learn power usage profiles of other customers, or cheat to gain undeserved rewards.

There may be external attackers who launch denial-of-service attack, man-in-the-middle attack, or eavesdrop. However, addressing these attacks is beyond the scope of this paper.

C. System Flow

The scheme includes the following processes. In the registration process, the DRP creates two accounts for a customer, one associated with his real identity and the other associated with his pseudonym. The real identity can be any information that uniquely identifies the customer, such as the account number or telephone number. Since a customer can only enroll in a single IDR program at a time, the DRP needs to make sure that a customer does not register multiple pseudonyms. This is achieved with the anonymous ticket: the customer obtains a ticket when he registers the real identity and presents it to the DRP when he anonymously registers the pseudonym. In the metering process, the smart meter collects metering data, constructs signatures on them, and sends them together with its pseudonym to the DRP through the anonymous channel. The DRP stores the data by pseudonym in the database and analyzes the data for operational and settlement purposes. The ICS signature ensures the authenticity of the metering data, while the ZKP ensures that adversaries cannot change the pseudonym in the message. The ZKP also enables customers to prove ownership of their pseudonyms when making personal inquiries for CBLs or metering data in the querying process. Customers claim rewards with a partially blinded signature (BBS+) which hides the real identity but ensures the integrity in the settlement process. The pseudo accounts of customers are revoked in the revocation process when customers leave the DRP programs.

D. Design Goals

We intend to design a scheme that guarantees privacy, integrity, and availability.

1) Privacy: Customers need to register their real identities for security reasons. However, they want to remain anonymous when querying their metering data or claiming their rewards. We guarantee this by allowing no other party except the customer himself to know his fine-grained power usage profile.

2) Integrity: We also need to ensure the integrity of the scheme. Misbehaviors such as falsifying the metering data or double spending should be detected immediately.

3) Availability: Guaranteeing the availability of IDR programs means that all the features required by IDR programs are fulfilled and the efficiency is guaranteed. Specifically, the DRP can gather information to profile, reward, and provide feedback to customers while customers can learn their DR performance and claim their rewards. Moreover, since the metering data should be transmitted and processed with low latency, the metering process should have low computation and communication overhead.

IV. Basic Protocol Design

We describe the basic protocols in this section. Due to page limit, we leave the detailed construction of the protocols and ZKPs in our technical report [18]. The DRP plays the role of the PKG and sets up the master key and public parameters for the ICS scheme and the BBS+ scheme as described in Section II.

A. Registration Process

Fig. 3 describes the registration process. The customer reveals his identity I to the DRP for registration. After verifying his eligibility, the DRP computes and sends the public/private key pair (Q'_I, S_I) (ICS signature) to the smart meter of the customer. Moreover, the customer commits a random secret s and sends commitment $\mathrm{CM}(s)$ to the DRP. The DRP then creates and returns δ_s^{RG}, a BBS+ signature on s, where label "RG" denotes registration ticket. The value of s remains hidden during the process. After the customer receives δ_s^{RG}, he stores $(\delta_s^{\mathrm{RG}}, s)$ as the registration ticket for his pseudonym.

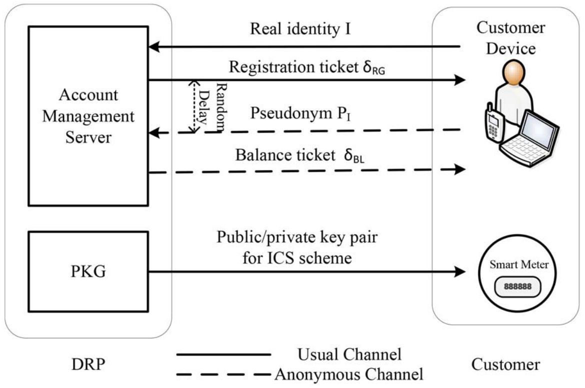


Fig. 3. Registration process.

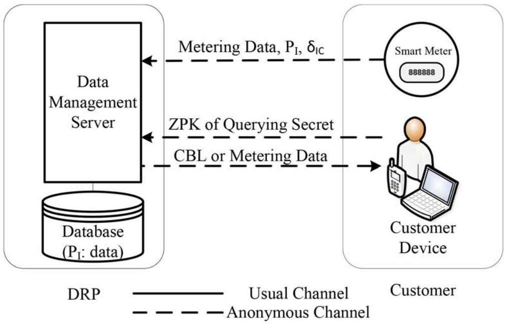


Fig. 4. Metering and querying process.

The customer also registers a pseudonym. To this end, the customer selects a random number λ_I as his secret and computes his pseudonym P_I as $P_I = g_4^{\lambda_I}$. After a random delay, the customer sends P_I and $(\delta_s^{\mathrm{RG}}, s)$ to the DRP through an anonymous channel. He proves to the DRP that (1) δ_s^{RG} is a valid signature on s, and (2) $P_I = g_4^{\lambda_I}$ with a ZKP PK_1

$$\mathrm{PK}_1\Big\{\big(\lambda_I, A, c, z, I, z'\big) : P_I = g_4^{\lambda_I} \wedge \hat{e}\big(A, \omega g^c\big) = \hat{e}\big(g g_0^z g_1^I g_3^s, g\big)\Big\}. \quad (1)$$

If the DRP verifies the validity of the ZKP, it establishes a pseudo account associated with P_I. To initiate the balance in the pseudo account, the customer randomly selects a new value of s, sends commitment $\mathrm{CM}(I, B, s)$ to the DRP via the anonymous channel, and obtains δ_s^{BL}, a BBS+ signature on (I, B, s), where label "BL" denotes balance ticket. Here, B denotes the balance and is initialized to 0. The customer stores $(\delta_s^{\mathrm{BL}}, I, B, s)$ as the balance ticket. Note that s is updated every time, and hence a customer cannot use the same ticket twice.

After the registration of pseudonym P_I, the customer inputs the pseudonym into the smart meter. The smart meter stores the pseudonym locally and only uses the pseudonym for metering purposes.

B. Metering and Querying Processes

Fig. 4 describes the metering and querying processes. At each reporting cycle t, the smart meter collects metering data m_t and generates an ICS signature δ_{IC} on the metering data. It then attaches the pseudonym of the customer to

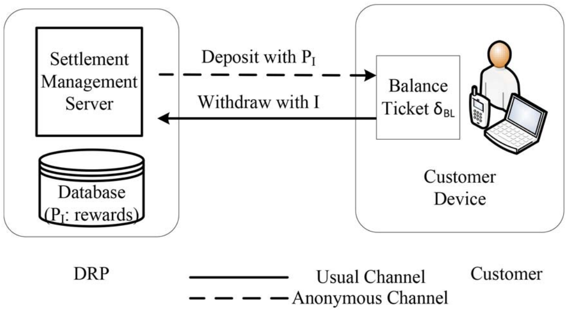


Fig. 5. Settlement process.

the message and sends the entire message $(m_t, t, P_I, \delta_{\mathrm{IC}})$ to the DRP through the anonymous channel. Upon receiving the message, the DRP checks the validity of δ_{IC}. If δ_{IC} passes the verification, the DRP stores $(m_t,\ \delta_{\mathrm{IC}})$ as the metering record at time t for the pseudo account P_I. Otherwise, the DRP discards the message. The metering records associated with P_I can be used to calculate individual CBL and allocate DR rewards.

In the querying process, the customer proves his knowledge about the secret key λ_I of pseudo account P_I with a ZKP PK$_2$

$$\mathrm{PK}_2\left\{\lambda_I : P_I = g_4^{\lambda_I}\right\}. \tag{2}$$

The customer sends a querying request together with PK$_2$ to the DRP via the anonymous channel. If PK$_2$ is correctly constructed, the DRP locates the requested data in the database and sends it back over the established anonymous channel. Otherwise the request is rejected and the corresponding request is ignored.

C. Settlement Process

The DR rewards are allocated to pseudo accounts by the DRP-based on individual curtailments. Customers may claim their rewards in two steps, as described in Fig. 5. First, a customer adds the reward into his balance ticket through the anonymous channel. Suppose his old balance ticket is $(\delta_{\tilde{s}}^{\mathrm{BL}}, I, \tilde{B}, \tilde{s})$. To transfer reward d from the pseudo account, the customer first checks if the reward in his pseudo account is larger than d. If yes, he selects a random secret s and sends commitment $\mathrm{CM}(s, I, B, \tilde{B})$ to the DRP, together with the following ZKP PK$_3$:

$$\mathrm{PK}_3\left\{\left(\lambda_I, \tilde{A}, \tilde{c}, I, \tilde{z}, \tilde{B}, \tilde{s}\right) : P_I = g_4^{\lambda_I} \wedge B - d > 0 \right.$$
$$\left. \wedge\, C = g_0^{z'} g_1^{I} g_2^{\tilde{B}} g_3^{s} \wedge \hat{e}\left(\tilde{A}, \omega g^{\tilde{c}}\right) = \hat{e}\left(g g_0^{\tilde{z}} g_1^{I} g_3^{\tilde{s}}, g\right)\right\}$$

which shows that his pseudonym is P_I, the new balance is positive, and the balance ticket is correctly formed. Now the DRP verifies if both $\tilde{s}$ is never shown before and PK$_3$ is true. If yes, it replies with a new BBS+ signature δ_s^{BL} on the tuple (I, B, s). The customer stores $(\delta_s^{\mathrm{BL}}, I, B, s)$ as the new balance ticket.

Second, the customer redeems reward from the balance ticket with his real identity. The customer selects a new s and sends the balance ticket $\delta_{\tilde{s}}^{\mathrm{BL}}$, the withdrawal amount d, and a ZKP PK$_4$ to the DRP, which is a combination of PK$_2$ and PK$_3$. The DRP then verifies the validity of PK$_4$ and checks if $\tilde{s}$ is never used before. If both are true, it returns a new BBS+ signature δ_s^{BL} on (I, B, s) and the customer stores $(\delta_s^{\mathrm{BL}}, I, B, s)$ as the new balance ticket.

D. Revocation Process

When the customer quits from an IDR program, the DRP needs to ensure that both the identifiable and the pseudo accounts of the customer are closed. This is guaranteed through a revocation ticket. When the customer revokes the pseudo account through the anonymous channel, he obtains a revocation ticket δ_s^{RV} from the DRP. The revocation ticket contains a BBS+ signature on (I, s) with s being the random secret selected by the customer. After a random period, the customer presents his real identity, the revocation ticket, and a ZKP PK$_5$ together to the DRP, where

$$\mathrm{PK}_5\left\{\left(A, c, z, I, z'\right) : \hat{e}\left(A, \omega g^{c}\right) = \hat{e}\left(g g_0^{z} g_1^{I} g_3^{s}, g\right)\right\}.$$

This ticket proves the revocation of the pseudo account associated with customer I. Then, the DRP can continue to complete the rest of the revocation process.

V. Practical Considerations and Extensions

In this section, we discuss some practical issues and provide useful extensions to solve them.

A. Cloaking Mechanism

In the metering process, all the metering records of a customer are associated with the same pseudonym, which enables the DRP to link the metering data and perform basic operations. In theory, the DRP only knows the pseudonym of the power usage profiles, and thus the real identity of the customer is hidden. In practice, however, the DRP may still infer the real identity of the customer by mining the relationships between rewards and withdrawals. For example, if a customer withdraws all the available rewards in his account every settlement cycle, the withdrawals will equal the rewards. The DRP can then use the rewards as a quasi-identifier to find the real identity associated with the pseudo account. To avoid such a linkage, customers can use cloaking mechanisms when they withdraw from the balance tickets.

In general, the cloaking rules hide the relationship between withdrawals and rewards by reducing the withdrawal amount and frequency. Ideally, if a customer withdraws once per year and leaves some balance unredeemed, the DRP can only learn an estimate of his total reward through the year. This information does not reveal the relationship between the real identity and the pseudonym since it applies to many customers. However, customers usually want to use rewards whenever they are available, and redeeming rewards motivates them to be more active in future DR events. Hence, we need to balance privacy and timeliness.

In the following, we propose two cloaking mechanisms, i.e., floor function withdrawal (FFW) mechanism and partition and random selection (PRS) mechanism. Without loss of generality, we assume that withdrawal decisions are made once per settlement cycle.

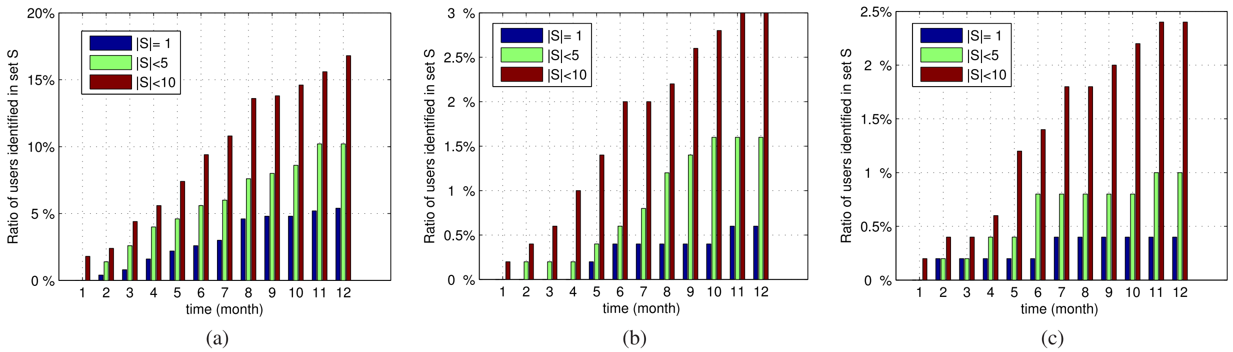


Fig. 6. Anonymity for (a) FFW with $p = 0.2$, (b) PRS with $p = 0.2$, and (c) PRS with $p = 0.5$.

The FFW divides the range of rewards into nonoverlapping intervals. Each customer falls into one interval based on their remaining balance in the balance ticket. At the end of a settlement cycle, a customer withdraws the floor value of his interval. In this way, customers in the same interval are indistinguishable because they withdraw the same amount of rewards. The achieved anonymity is determined by interval size: intervals of larger size may include more customers, and therefore provide stronger anonymity guarantee. Intervals do not need to be of the same size. For intervals which contain a dense population, the size can be chosen smaller, while for other intervals, the size should be larger.

The PRS defines a set of cells, say $\{5, 10, 20, 40\}$. Customers first partition the rewards into cells. Then they select each cell with a probability p and withdraw an amount equal to the sum of the selected cells. For example, if the reward is 45, the customer may divide it into $\{5, 10, 10, 20\}$, choose a subset of it with selection probability 0.8, and finally select cells $\{5, 10, 10\}$. The withdrawal is the sum of these cells, which is 25.

B. Pseudonym Update

Cloaking schemes can reduce information leaked to the DRP. However, in the long run, the DRP can still gain enough information for de-anonymization. Suppose that Alice receives rewards $R_1, R_2, \ldots, R_N$ and withdraws $W_1, W_2, \ldots, W_N$ in the first N settlement cycles. The DRP learns that

$$\sum_{k=1}^{n} W_k \leq \sum_{k=1}^{n} R_k, n = 1, 2, \ldots, N \tag{3}$$

where W_k is the kth withdrawal and R_k is the kth reward of Alice. If the withdrawals of customer Bob also satisfy (3), that is

$$\sum_{k=1}^{n} W_k \leq \sum_{k=1}^{n} R'_k, n = 1, 2, \ldots, N \tag{4}$$

where R'_k is the kth reward of Bob, then Alice and Bob are indistinguishable from the DRP side. However, as N becomes large, it becomes harder to find a "Bob" who is indistinguishable from Alice. With cloaking mechanisms, customers can slow down this process but not stop it. Hence, Alice needs to update the pseudonym after a few settlement cycles. Updating the pseudonym includes revocation of current pseudonym (Section IV-D) and registration of the new one (Section IV-A). To avoid linkage of the two pseudonyms, after revocating the old one, the customer waits a certain period before registering the new pseudonym.

C. Reidentification

There are scenarios where the customer needs to provide his power usage profiles to others. For example, a customer may use his power usage profile to justify in a legal dispute. This is especially important when the DRP is not a third party, but the utility company itself. In this case, the DRP should enable the customer to prove ownership of his profile. In other words, the customer should be able to prove to the DRP or other parties that the power usage profile is linked to his real identity. This feature can be provided through the ICS scheme.

To prove his ownership of a metering record, the customer presents the secret λ_I together with the metering data, corresponding ICS signatures, and the real identity I to the verifier. The verifier parses the ICS of the metering data in the record as $\delta_{\mathrm{IC}} = (Q, Q', U, V)$, computes the public key for the customer as $Q_I = H_1(I)$, and checks if $Q_I = \lambda_I^{-1} Q$ holds. If the result is yes, then the verifier is convinced that the signed metering data is generated by the customer with identity I. Hence, the customer with identity I is reidentified to be the owner of the power usage profile.

Since the DRP already knows the linkage between the pseudonym P_I and the metering data, it can now readily link the real identity to the pseudonym. If a customer wants to keep his future power usage profile hidden after the reidentification process, he needs to update his pseudonym following the update protocol in Section V-B.

VI. Security and Privacy Analysis

In this section, we show that the proposed scheme achieves the security goals of integrity and privacy and analyze the unlinkability achieved though our cloaking mechanism.

A. Data Integrity

Data integrity of the proposed scheme is guaranteed in the following aspects.

1) Defending Cheating Customers: We model the interaction between a cheating user $\mathcal{A}$ and an honest DRP $\mathcal{C}$ as a game. Let the DRP $\mathcal{C}$ record the balance B remained in

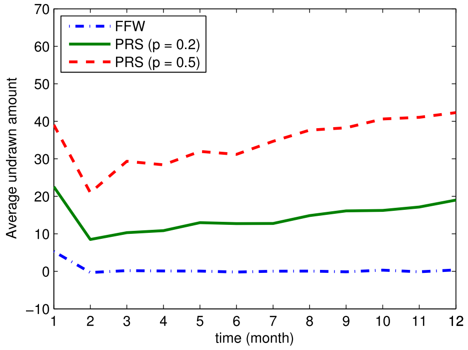


Fig. 7. Evaluation of cloaking mechanisms.

the account of $\mathcal{A}$. $\mathcal{A}$ wins the game if $\mathcal{A}$ can get a negative balance of B. We use reduction argument for our proof. Specifically, we show that if adversary $\mathcal{A}$ can win the game, then a forgery attack can be constructed against the BBS+ signature. However, BBS+ signature has been shown to be unforgeable in [16]. Thus, there does not exist such adversary $\mathcal{A}$. In other words, cheating customers cannot win in our system. Due to space limit, we leave the detailed formal proof in our technical report [18].

2) Authenticity: The authenticity of the metering data, ensured by the ICS scheme, allows the DRP to verify that the data are generated by a genuine and registered smart meter. No attackers can forge or tamper the metering data since they cannot forge the ICS under adaptively chosen message attack [10]. Tickets are used in our scheme for registration process, revocation process, and settlement process. The tickets, or BBS+ signatures, have been proven to be secure against existential attack [16]. Hence, attackers cannot forge tickets to gain monetary benefits. Besides, the attackers are not able to replay used tickets as the secret s in the ticket is updated whenever it is shown to the DRP, and the DRP can easily determine whether a ticket has been used or not by looking it up in the database.

3) Confidentiality: In addition to protocols we described in this paper, standard asymmetric and symmetric encryptions are used to provide confidentiality. For normal communication, either encryption scheme is good. For anonymous communication, asymmetric encryption schemes are required. For example, in the metering process, smart meters need asymmetric encryption to ensure confidentiality. To this end, they encrypt messages with the public key of the DRP, who then decrypts them with its private key. This ensures end-to-end confidentiality of the metering data.

B. Privacy

We preserve customer privacy by ensuring the anonymity of fine-grained metering data. Each customer registers both a real identity and a pseudonym, and only pseudonyms are attached to metering data. The DRP can neither infer the real identities from the metering data in the metering process nor link real identities and pseudonyms in other processes.

1) Privacy in Registration, Querying, Settlement, and Revocation: We use a game to model user privacy in registration, querying, settlement, and revocation. Let the curious DRP interact with $\mathcal{C}$ who acts on behalf of two users. User privacy is provided in these processes if the DRP cannot tell which of the two users is responsible for a particular interaction under the condition that all other interactions have been identified by the curious DRP. The particular interaction could be during pseudonym registration, settlement, querying, and revocation, but not during real identity registration, because real identity is to be known in real identity registration. Our definition also guarantee that the interactions cannot be linked. Due to space limit, we include the details of the proof in our technical report [18]. In the following, we provide an intuitive description of the privacy guarantee provided by our scheme.

In the registration process, BBS+ signatures are used to hide the relationship between the real identity and the pseudonym. A customer obtains a BBS+ signature (i.e., the registration ticket in Section IV) after he registers his real identity. In a separate communication session, the customer uses this signature to prove his eligibility of enrollment and to register his pseudonym. Since the BBS+ signature hides the value of the real identity, the DRP does not know his real identity when registering the pseudonym and thus cannot link these two identities. The same conclusion can be given for the settlement process and the revocation process. In the querying process, customers inquire their data through pseudonyms and no information of real identity is involved.

Since information involving pseudonyms is sent through a proxy who hides the static physical address of a smart meter from the DRP, anonymity is also ensured in the physical layer.

2) Anonymity in Metering: During the metering process, smart meters only attach pseudonyms to metering data. To verify the authenticity of the metering data, they sign the metering data with ICS. The secret value μ of the ICS is stored locally at the smart meter, and the DRP does not know it. Hence, due to the anonymity property of the ICS, the DRP can verify the data source, but it cannot identify the customer [10].

C. Unlinkability Between Pseudo Accounts and Identifiable Accounts

In Section V, we show that the relationship between rewards and withdrawals may compromise anonymity and propose two cloaking mechanisms to mitigate the attack. The cloaking mechanisms divide customers into several sets and customers in the same set are indistinguishable. Denote the set as S. A set with larger size provides stronger anonymity.

Suppose the DRP has 500 subscribed customers and customers withdraw money once per settlement cycle (e.g., a month). We assume that DR rewards follow a Gaussian distribution with mean 50 and variance 20. We simulate the withdrawal behaviors of customers with the FFW mechanism, and the PRS mechanism under two parameter settings: 1) PRS with cells $\{1, 5, 10, 50\}$ and probability $p = 0.2$, and 2) PRS with cells $\{1, 5, 10, 50\}$ and probability $p = 0.5$. We demonstrate the ratio of customers with different sizes of S in Fig. 6.

TABLE I
NUMBER OF PAIRING AND EXPONENTIATION OPERATIONS

	Registration		Metering			Querying		Settlement	
	Customer	DRP	Customer	Smart Meter	DRP	Customer	DRP	Customer	DRP
Group $\mathbb{G}$ exponentiation (pre-processed)	22	14	0	0	0	2	1	48	21
Group $\mathbb{G}$ exponentiation (direct)	1	6	0	0	0	0	1	3	9
Group $\mathbb{G}_T$ exponentiation (pre-processed)	4	6	0	0	0	0	5	13	16
Group $\mathbb{G}_T$ exponentiation (direct)	1	2	0	0	0	0	1	2	3
Pairing (one parameter is constant)	3	2	0	0	5	0	1	6	2
Pairing (both parameters are not constant)	2	0	0	0	0	0	0	2	0

Overall, most of the customers are indistinguishable at least from nine others. However, as the DRP gradually gains more information, the sets are becoming smaller, and customers need to update their pseudonyms. We compare their average undrawn amounts on a monthly basis in Fig. 7. We can see that the FFW mechanism requires the fewest amount of undrawn rewards among all the three approaches, while the PRS mechanism with selection probability $p = 0.5$ requires the most. This illustrates the tradeoff between privacy and timeliness: if you want better privacy, you should withdraw less frequently.

VII. Performance Analysis

In this section, we analyze the efficiency and cost of the proposed scheme. The computation cost comes mainly from pairings and exponentiations in signature schemes (ICS, BBS+) and ZKP (PK_1–PK_5). We summarize number of these two operations in basic protocols for smart meters, customers, and the DRP in Table I.

From this table, we can see that smart meters do not need to perform any of the two operations. The most time-consuming processes performed by smart meters are ICS generation in the metering process, which involves no paring or exponentiation operations and can be handled by existing smart meters efficiently. The customer devices or DRP servers are assumed to be powerful enough to conduct computation-intensive operations. Nonetheless, some of the operations, such as the exponentiations that have constant base (e.g., $g_0^{z'}$) and the pairings with one of the parameter being constant [e.g., $\hat{e}(gg_0^z g_1^I g_3^s, g)$], can be preprocessed, which expedites the calculation greatly.

Based on the simulation results of [19] that uses similar cryptographic tools, we can estimate the computation time of our algorithm. If we use a smartphone HTC Desire HD with QSD8255 1 GHz CPU and 1.5 GB ROM to simulate the customer device, the registration time for the customer is less than 3 s, and the settlement time is less than 6 s. If we use a desktop with Q6600 2.4 GHz CPU and 3 GB RAM as the server of DRP, the registration time for the DRP is 0.2 s, the metering time is 0.05 s, and the settlement time is 0.3 s. Since registration and billing processes happen at low frequency, the processing time in the order of a few seconds is insignificant. Since smart meters are not involved in any computation intensive operations such as exponentiation or pairing operations, our proposed protocols can be implemented efficiently.

VIII. Related Work

While instrumental to the implementation of DR, fine-grained metering data collected by the AMI can be used to determine occupant activities, raising serious privacy concerns [20]. Research studies on nonintrusive load monitoring [6], [21], [22] have shown the possibility of deducing appliance usage patterns from fine-grained metering data. The appliance usage patterns can be further analyzed to learn the health status, daily routines, or unusual behaviors such as "you slept late at night" and "your child is left alone at home" [7]. Hence, a growing number of research activities have been carried out to address privacy issues in the AMI.

The approaches to address privacy issues in the AMI can be divided into three categories. The first category proposes to aggregate individual metering data before sending them out to utility companies since most benefits of the smart grid can be achieved with the aggregate data. Aggregation can be either performed at a central point [23]–[25] or distributed in the network [26]. The second category uses cryptographic tools to hide sensitive information, mainly adopted for private billing purposes in PDR programs [7], [24], [27]. These works intend to calculate bills at the customer side and ask customers to prove the correctness of their bills to utilities. The third category uses anonymity to protect user privacy [28]. The aforementioned approaches share a common assumption: metering data for operational purposes do not need to be attributable to a specific customer, and metering data for billing purposes do not require to be in fine granularity. This assumption, however, no longer holds for IDR programs. Fine-grained metering data are required when the DRP schedules demand curtailments, calculates CBLs, and allocates DR rewards for individual customers. Hence, both fine granularity and attributability are required for IDR programs. In this case, aforementioned privacy protection mechanisms such as aggregation are not applicable, and a new approach is needed.

Anonymous credentials have been proposed to preserve privacy in [29] and [30]. Specifically, a user obtains a credential from an issuer and demonstrates the possession of the credential to a verifier who only has the public information of the issuer. The verifier can learn nothing beyond the fact that the user owns a credential granted by the issuer, even when it colludes with the issuer. "ANONIZE" [31] is an anonymous survey system where users can create an anonymous single-use token (or credential) and use it to answer a given survey. However, single-use token fails to serve the billing purpose in our scenario, where the balance should be inherited and updated repeatedly across different settlement cycles. On the other hand, "OPAAK" [32] provides an authentication framework with privacy-preserving and single sign-on properties. This is similar to our solution, however, besides identity management, our scenario also requires management of a running balance and authentication of metering data which can not be addressed by their work.

IX. Conclusion

In this paper, we have identified and addressed the unique privacy issues in IDR programs. We have proposed a scheme which provides fine-grained metering data to the DRP for basic operations, ensuring data integrity throughout all the processes. The scheme protects customer privacy by separating the real identity and the fine-grained metering data, i.e., the DRP can only learn either the real identity or the fine-grained metering data at a time but cannot link them together. In the case when reidentification is required, the linkage between real identity and metering data can be easily restored. Hence, our scheme provides an integrated solution for privacy-aware IDR programs, which promotes the acceptance of IDR programs.

References

[1] *Benefits of Demand Response in Electricity Markets and Recommendations for Achieving Them*, U.S. Dept. Energy, Washington, DC, USA, Tech. Rep., Feb. 2006.

[2] A. Ipakchi and F. Albuyeh, "Grid of the future," *IEEE Power Energy Mag.*, vol. 7, no. 2, pp. 52–62, Mar./Apr. 2009.

[3] C. Goldman, M. Reid, R. Levy, and A. Silverstein, "Grid of the future," Lawrence Berkeley Nat. Lab., Univ. California, Berkeley, CA, USA, Tech. Rep. LBNL-55281, 2010.

[4] EnerNoc. (2008). *The Demand Response Baseline*. [Online]. Available: http://www.naesb.org/pdf4/dsmee_group2_022609w2.pdf

[5] G. W. Hart, "Non-intrusive appliance load monitoring," *Proc. IEEE*, vol. 80, no. 12, pp. 1870–1891, Dec. 1992.

[6] D. C. Bergman *et al.*, "Distributed non-intrusive load monitoring," in *Proc. IEEE PES Innov. Smart Grid Technol. (ISGT)*, Anaheim, CA, USA, 2011, pp. 1–8.

[7] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in *Proc. ACM Workshop Embedded Sens. Syst. Energy Efficien. Build.*, Zurich, Switzerland, 2010, pp. 61–66.

[8] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*. Berlin, Germany: Springer, 1985, pp. 47–53.

[9] J. C. Cha and J. H. Cheon, "An identity-based signature from gap Diffie–Hellman groups," in *Public Key Cryptography—PKC 2003*. Berlin, Germany: Springer, 2002, pp. 18–30.

[10] C.-K. Chu and W.-G. Tzeng, "Identity-committable signatures and their extension to group-oriented ring signatures," in *Information Security and Privacy*. Berlin, Germany: Springer-Verlag, 2007, pp. 323–337.

[11] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM J. Comput.*, vol. 18, no. 1, pp. 186–208, 1989.

[12] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Proc. Adv. Cryptol. (CRYPTO)*, Santa Barbara, CA, USA, 1987, pp. 186–194.

[13] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," in *Proc. Adv. Cryptol. (CRYPTO)*, Santa Barbara, CA, USA, 1997, pp. 410–424.

[14] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Proc. Annu. Int. Cryptol. Conf. (CRYPTO)*, Santa Barbara, CA, USA, 1992, pp. 129–140.

[15] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Proc. Annu. Int. Cryptol. Conf. (CRYPTO)*, Santa Barbara, CA, USA, 2004, pp. 41–55.

[16] M. H. Au, W. Susilo, and Y. Mu, "Constant-size dynamic k-TAA," in *Proc. 5th Int. Conf. Security Cryptogr. Netw.*, Maiori, Italy, 2006, pp. 111–125.

[17] K. Coughlin, M. A. Piette, C. Goldman, and S. Kiliccote, "Estimating demand response load impacts: Evaluation of baseline load models for non-residential buildings in California," Lawrence Berkeley Nat. Lab., Berkeley, CA, USA, Tech. Rep. LBNL-63728, 2008.

[18] Y. Gong, Y. Cai, Y. Guo, and Y. Fang. (2014). *A Privacy-Preserving Framework for Incentive-Based Demand Response in the Smart Grid*. [Online]. Available: http://www.fang.ece.ufl.edu/drafts/PrivacyIDR-extended.pdf

[19] J. K. Liu, M. H. Au, W. Susilo, and J. Zhou, "Enhancing location privacy for electric vehicles (at the right time)," in *Proc. 17th Eur. Symp. Res. Comput. Security (ESORICS)*, Pisa, Italy, 2012, pp. 397–414.

[20] E. Quinn, "Smart metering and privacy: Existing laws and competing policies," *SSRN 1462285*, 2009.

[21] S. McLaughlin, P. McDaniel, and W. Aiello, "Protecting consumer privacy from electric load monitoring," in *Proc. 18th ACM Conf. Comput. Commun. Security (CCS)*, Chicago, IL, USA, 2011, pp. 87–98.

[22] M. A. Lisovich, D. K. Mulligan, and S. B. Wicker, "Inferring personal information from demand-response systems," *IEEE Security Privacy*, vol. 8, no. 1, pp. 11–20, Jan./Feb. 2010.

[23] F. D. Garcia and B. Jacobs, "Privacy-friendly energy-metering via homomorphic encryption," in *Security and Trust Management*. Berlin, Germany: Springer-Verlag, 2011, pp. 226–238.

[24] K. Kursawe, G. Danezis, and M. Kohlweiss, "Privacy-friendly aggregation for the smart-grid," in *Proc. 11th Int. Conf. Privacy Enhanc. Technol.*, Berlin, Germany, 2011, pp. 175–191.

[25] Z. Erkin and G. Tsudik, "Private computation of spatial and temporal power consumption with smart meters," in *Proc. 10th Int. Conf. Appl. Cryptogr. Netw. Security*, Berlin, Germany, 2012, pp. 561–577.

[26] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Gaithersburg, MD, USA, 2010, pp. 327–332.

[27] A. Rial and G. Danezis, "Privacy-preserving smart metering," in *Proc. 10th ACM Workshop Privacy Elect. Soc.*, Chicago, IL, USA, 2011, pp. 49–60.

[28] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Gaithersburg, MD, USA, 2010, pp. 238–243.

[29] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete," *Commun. ACM*, vol. 28, no. 10, pp. 1030–1044, 1985.

[30] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2001, pp. 93–118.

[31] S. Hohenberger, S. Myers, and R. Pass, "ANONIZE: A large-scale anonymous survey system," in *Proc. 2014 IEEE Symp. Security Privacy*, Oakland, CA, USA, pp. 375–389.

[32] G. Maganis, E. Shi, H. Chen, and D. Song, "OPAAK: Using mobile phones to limit anonymous identities online," in *Proc. 10th Int. Conf. Mobile Syst. Appl. Serv.*, Ambleside, U.K., 2012, pp. 295–308.

Yanmin Gong (S'10) received the B.Eng. degree in electronics and information engineering from the Huazhong University of Science and Technology, Wuhan, China, and the M.S. degree in electrical engineering from Tsinghua University, Beijing, China, in 2009 and 2012, respectively. She is currently pursuing the Ph.D. degree in electrical and computer engineering from the University of Florida, Gainesville, FL, USA.

Her current research interests include cybersecurity and privacy in mobile computing, mobile health, big data, and cyber-physical systems.

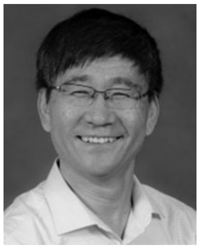
Ying Cai (M'14) received the B.S. degree from Xidian University, Xi'an, China; the M.S. degree from the Beijing University of Science and Technology, Beijing, China; and the Ph.D. degree from Beijing Jiaotong University, Beijing, in 1989, 1992, and 2010, respectively, all in applied mathematics and information security.

She is currently a Full Professor with the Beijing University of Information Science and Technology, Beijing. From 2012 to 2013, she was a Visiting Research Scholar with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, USA. Her current research interests include cybersecurity, wireless networks, and cryptographic algorithms and analysis. She has authored and co-authored over 30 papers in refereed professional journals and conferences.

Yuanxiong Guo (M'14) received the B.Eng. degree in electronics and information engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2009, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Florida, Gainesville, FL, USA, in 2012 and 2014, respectively.

Since 2014, he has been an Assistant Professor with the School of Electrical and Computer Engineering, Oklahoma State University, Stillwater, OK, USA. His current research interests include smart grids, sustainable computing and networking systems, big data, and cyber-physical systems security and privacy.

Dr. Guo was a recipient of the Best Paper Award from the IEEE Global Communications Conference in 2011.



Yuguang Fang (F'08) received the M.S. degree in mathematics from Qufu Normal University, Shandong, China, in 1987, and the Ph.D. degrees in systems engineering from Case Western Reserve University, Cleveland, OH, USA, and electrical engineering from Boston University, Boston, MA, USA, in 1994 and 1997, respectively.

From 1998 to 2000, he was with the Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ, USA, as an Assistant Professor. He then joined the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, USA, as an Assistant Professor in 2000, where he received an early promotion to Associate Professor with tenure in 2003, and then to Full Professor in 2005. He held the University of Florida Research Foundation Professorship from 2006 to 2009, a Changjiang Scholar Chair Professorship with Xidian University, Xi'an, China, from 2008 to 2011, and a Guest Chair Professorship with Tsinghua University, Beijing, China, from 2009 to 2012. He has published over 400 papers in refereed professional journals and conferences.

Dr. Fang was a recipient of the U.S. National Science Foundation Faculty Early Career Award in 2001, the U.S. Office of Naval Research Young Investigator Award in 2002, the IEEE Communications Society Wireless Communications Technical Committee Recognition Award, the Best Paper Award from the IEEE Globecom in 2011, the IEEE International Conference on Network Protocols in 2006, the IEEE TCGN at the IEEE High-Speed Networks Symposium, and the IEEE Globecom in 2002. He was also the recipient of the 2010–2011 UF Doctoral Dissertation Advisor/Mentoring Award, the 2011 Florida Blue Key/UF Homecoming Distinguished Faculty Award, and the 2009 UF College of Engineering Faculty Mentoring Award. He has been serving as an Editor-in-Chief of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY since 2013. He also served as an Editor-in-Chief of the IEEE WIRELESS COMMUNICATIONS from 2009 to 2012 and serves/served on several editorial boards of technical journals including the IEEE TRANSACTIONS ON MOBILE COMPUTING from 2003 to 2008 and from 2011, the IEEE NETWORK from 2012, the IEEE TRANSACTIONS ON COMMUNICATIONS from 2000 to 2011, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2002 to 2009, the *IEEE Journal on Selected Areas in Communications* from 1999 to 2001, the *IEEE Wireless Communications Magazine* from 2003 to 2009, and *Wireless Networks* from 2001. He also served on the Steering Committee of the IEEE TRANSACTIONS ON MOBILE COMPUTING from 2008 to 2010. He has been actively participating in professional conference organizations, such as the Technical Program Co-Chair for the IEEE INOFOCOM'14, the Steering Committee Co-Chair for QShine from 2004 to 2008, the Technical Program Vice-Chair for the IEEE INFOCOM'05, the Technical Program Area Chair for the IEEE INFOCOM from 2009 to 2013, the Technical Program Symposium Co-Chair for the IEEE Globecom'04, and the Technical Program Committee Member of the IEEE INFOCOM in 1998, 2000, and from 2003 to 2008.