Cost-Friendly Differential Privacy for Smart Meters: Exploiting the Dual Roles of the Noise

Zijian Zhang, *Member, IEEE*, Zhan Qin, *Member, IEEE*, Liehuang Zhu, *Member, IEEE*, Jian Weng, *Member, IEEE*, and Kui Ren, *Fellow, IEEE*

***Abstract*—Smart meters have been widely installed to monitor residential electricity usage worldwide. This brings a serious privacy challenge for the customers, because the meter readings can possibly expose their activities in the house. To address this privacy issue, battery-based privacy preserving schemes have already been studied for several years. In these schemes, a rechargeable battery can both prevent the meter readings from leaking the customer's energy consumption and play a role of saving the cost. However, to the best of our knowledge, none of the existing schemes can achieve differential privacy and cost saving simultaneously. In this paper, we first propose a battery-based differential privacy-preserving (BDP) scheme. We further present two cost-friendly differential privacy-preserving (CDP) schemes by extending BDP scheme. Simulation analyses show that the privacy loss of both CDP schemes are smaller than the existing works. Meanwhile, both CDP schemes stably save the cost under multiple pricing policies.**

***Index Terms*—Differential privacy, cost saving, smart meter, battery, pricing policy.**

I. Introduction

ELECTRIC companies have been installing smart meters all around the world, with the development of smart grid. In the United States, more than eight million smart meters have already been installed [1]. In Europe, at least 80% of all consumers are estimated to install smart meters by 2020, according to the current national roll-out plans [2]. These smart meters monitor residential electricity usage information at minute-level or second-level incessantly [3]. On one hand, this information is necessary for the electricity companies to provide a secure and efficient power supply. For example, it is useful to notify outage [4] and reckon the total amount of energy consumption [5]. On the other hand, this information causes a serious threat to the customers' privacy [6] at the same time. The meter readings can possibly expose what types of electrical appliances are being used, thereby inferring the customer's behavior in the house [7]. The threat has led the customers to boycott smart meters. In California, nine cities have voted to make smart meters illegal in their communities [8].

To address the privacy issue, a rechargeable battery is installed to prevent the meter readings from leaking the customer's real energy consumption [9]. Specifically, after the battery is installed in the house, the meter readings only represent the total energy consumption from the electrical appliances and the battery. Since the charge-discharge rate of the battery is adjustable, the meter readings can be flattened [10]–[12] or randomized [13], [14] by selecting an appropriate rate. Therefore, the real energy consumption is hidden from the meter readings.

Besides privacy protection, the battery can also play a role of saving the customer's cost under Time-of-Use (TOU) pricing policy. Specifically, TOU pricing policy has been used to alleviate the electricity production and transmission pressure for the electricity companies [15]. The main idea of TOU pricing policy is to set the unit price at peaks time higher than that at the other times, in order to encourage customers to reduce the electricity demand at peak times. There are two kinds of pricing policies in smart grid. One is to stipulate all the unit prices in advance. Since the unit price at each time period is nonadjustable, it is named as static policy. The other just publicizes the lowest and highest unit price to the customer [16]. The electricity company can autonomously adjust the unit price at any time, due to the total energy consumption. This policy is regarded as dynamic policy [17]. Obviously, customer's bill can be reduced when the battery charges under a lower unit price and discharges under a higher unit price. Following this principle, several schemes have been proposed to save the cost for both static and dynamic policies [16], [18].

In recent years, the method of differential privacy is applied to define the customer's privacy in smart grid [13], [14]. This method supports formal proof to the privacy, when compared with the traditional information-theoretical methods, such as relative entropy [19] or mutual information [20]. In addition, customer's privacy can be guaranteed at about the same level if differential privacy is achieved. Unfortunately, to the best of our knowledge, none of the existing battery-based privacy preserving schemes can achieve differential privacy and save the cost simultaneously.

Manuscript received July 18, 2015; revised January 21, 2016 and April 26, 2016; accepted June 11, 2016. Date of publication June 28, 2016; date of current version February 16, 2017. This work was supported in part by the National Science Foundation under Grant CNS-1262275, Grant CNS-1262277, and Grant CNS-1318948, and in part by the National Natural Science Foundation of China under Grant 61271512 and Grant 61300177. Paper no. TSG-00841-2015. *(Corresponding author: Liehuang Zhu.)*

Z. Zhang and L. Zhu are with the Beijing Institute of Technology, Beijing 100081, China (e-mail: liehuangz@bit.edu.cn).

Z. Qin and K. Ren are with the Computer Science and Engineering Department, State University of New York at Buffalo, Buffalo, NY 14228 USA.

J. Weng is with Jinan University, Guangzhou 510632, China.

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.2016.2585963

We summarize our contributions as described below:

(1) We propose a battery-based differential privacy-preserving (BDP) scheme and formally prove its privacy.

(2) By extending BDP scheme, we present two cost-friendly differential privacy-preserving (CDP) schemes under static and dynamic pricing policies. Both CDP schemes are formally proved to achieve differential privacy and cost saving simultaneously.

(3) Using REDD dataset, we quantitatively evaluate the privacy leakage and cost for both CDP schemes under static and dynamic pricing policies in the experiments.

The rest of this paper is organized as follows. Section II reviews the related work. Section III briefly recalls the definition of differential privacy and multi-armed bandit problem. In Section IV, we describe the system model and the formal goal. Section V proposes the BDP scheme and two CDP schemes under static and dynamic pricing policies. In Section VI both CDP schemes are proved to achieve differential privacy and cost saving simultaneously. Section VII evaluates the privacy loss and cost saving for both CDP schemes and the existing works. Section VIII draws the conclusion.

II. Related Work

Some studies focus on the battery-based privacy protection in smart grid. Kalogridis *et al.* [10] are first to propose a best effort (BE) scheme. This scheme tries to set the meter readings as a fixed value. In this scheme, the rechargeable battery is used to bridge the gap between the customer's real energy consumption and the fixed value. Unfortunately, BE scheme is inevitable to expose the customer's privacy, because all the batteries have limited capacity and charge-discharge rate [11]. For example, the meter reading has to equal the energy consumption, when the energy left in the battery is too low or too high to make up the gap [11].

To resolve the problem, McLaughlin *et al.* [11] present a non-intrusive load leveling (NILL) scheme. In this scheme, the battery is set to charge/discharge when the capacity is too low/high to keep the fixed value. Yang *et al.* [12] introduce three lazy stepping (LS) schemes. The meter reading can be flexibly adapted, when the battery cannot keep the fixed value. Although NILL and LS schemes alleviate the exposure for the customer's energy consumption, both schemes cannot achieve differential privacy or cost saving [13].

Koo *et al.* [18] propose a wallet friendly privacy protection (PRIVATUS) scheme. This scheme uses dynamic programming to preserve privacy and reduce the bill under static policy. Yang *et al.* [16] design an optimal privacy preserving energy management (OPPEM) scheme. In OPPEM scheme, the variance of all the meter readings is minimized by using Lyapunov optimization. This scheme protects privacy and reduces the bill under dynamic policy [16]. However, both OPPEM and PRIVATUS schemes cannot achieve differential privacy [14].

Recently, Zhao *et al.* [13] propose a multitasking-BLH-exp3 (MBE) scheme. This scheme is proved to achieve differential privacy. However, the proof is not complete when the limited capacity and charge-discharge rate of the battery are considered. In addition, MBE scheme cannot cut down the bill.

III. The Preliminaries

A. Differential Privacy

We follow the definition of differential privacy in [21] as below.

Definition 1: A randomized function κ gives (ϵ, δ) differential privacy, if for all datasets D_1 and D_2 differing on at most one element, and all $S \subseteq Range(\kappa)$,

$$\Pr[\kappa(D_1) \in S] \le \exp(\epsilon) \times \Pr[\kappa(D_2) \in S] + \delta \tag{1}$$

where $Range(\kappa)$ denoted the range of the function κ.

Roughly, ϵ and δ are two parameters that quantitatively represent the privacy loss. The closer ϵ and δ approach to 0, the better privacy preserves.

Differential privacy can be achieved by adding a stochastic noise drawn from a Laplace distribution to the result of the query function [21]. Here the probabilistic density function of Laplace distribution is as follows [22].

$$pdf(x) = \frac{1}{2\sigma} e^{-|x-\mu|/\sigma}, x \in (-\infty, +\infty) \tag{2}$$

Here the parameter μ is often set to 0, and parameter σ has to be determined by the sensitivity which stands for the biggest impact of any element in the dataset on the result of the query function f [21]. The sensitivity is formally defined as below [22].

Definition 2: For $f : \mathcal{D} \to R^d$, the sensitivity of f is

$$\Delta f = \max_{D_1, D_2} \|f(D_1) - f(D_2)\| \tag{3}$$

for all D_1 and D_2 differing in at most one element.

To achieve differential privacy, σ should be no more than $\Delta f/\epsilon$ [21].

B. Multi-Armed Bandit Problem

Multi-armed bandit (MAB) problem has been widely studied in game theory, machine learning and economics. This problem formulates a strategy that allocates a sequential actions (arms) to maximize the total payoff in a series of experiments [23]. A famous dilemma in MAB problem is how a player chooses a proper arm to balance the exploitation and the exploration in the experiment, because the former performs well in the past, while the latter could bring more profit in the future [24]. To resolve this dilemma, the design of regret mechanism is critical and indispensable [23]. This mechanism evaluates the distance between the chosen arm and the optimal one. Formally, assume there are m arms. The payoff of each arm at time i is defined by $X_{j,i}$, where $j \in \{1, \dots, m\}$. If the arm I_j is chosen at time i, the corresponding profit $X_{I_j,i}$ can be earned. After we choose an arm for n times, the regret is defined as:

$$\mathcal{R}_n = \max_{j \in \{1,\dots,m\}} \sum_{i=1}^{n} X_{j,i} - \sum_{i=1}^{n} X_{I_j,i}. \tag{4}$$

IV. Models and Goals

A. System Model

The system model comprises (1) a smart meter, (2) a rechargeable battery, (3) a power controller that connects the

TABLE I
SUMMARY OF NOTATIONS

Smart Meter	
i	Time point.
$o(i)$	Meter readings at time i.
Rechargeable Battery	
$n(i)$	Charge-discharge rate of battery at time i
γ	Maximal discharge rate of battery.
η	Maximal charge rate of battery.
C	Capacity of the battery
$c(i)$	Energy left in the battery at time i.
Power Controller	
j	The sequence number for each electricity appliance.
d^i_j	The energy consumption for the j^{th} appliance at time i.
$\kappa(D_i)$	Customer's electricity consumption at time i.
α	The minimal consumption in all the electricity appliances.
β	The maximal consumption in all the electricity appliances.
Pricing Policy	
$p(i)$	Unit electricity price at time i.
p_{max}	The highest unit electricity price.
p_{min}	The lowest unit electricity price.

smart meter, the battery and the electrical appliances such as television, microwave or refrigerator in the house, and (4) a TOU pricing policy.

Here the notations of all the parameters in the system model are summarized in Table I. For the smart meter, i represents the time when the i^{th} report is sent. $o(i)$ is denoted as the meter reading at time i. For the rechargeable battery, the charge-discharge rate and the capacity of the battery at time i are represented by $n(i)$ and $c(i)$, respectively. Here $\gamma \leq n(i) \leq \eta$, $0 \leq c(i) \leq C$, and $c(i) = c(0) + \sum_{j=0}^{i} n(j)$. For the power controller, j stands for the sequence number of each electricity appliance in the house. Since each appliance may consume different energy at different time, d^i_j means the specific energy consumption for the j^{th} appliance at time i. $\kappa(D_i)$ denotes the customer's real energy consumption, and $\alpha \leq \kappa(D_i) \leq \beta$. In general, $\alpha \geq 0$, because $\kappa(D_i)$ is 0, when all the appliances are turned off. For the pricing policy, $p(i)$ represents the unit price at time i. p_{max} and p_{min} denote the highest and lowest unit price respectively. $p_{min} \leq p(i) \leq p_{max}$. Finally, we have $o(i) = \kappa(D_i) + n(i)$.

B. Adversarial Model

The adversary is curious-but-honest. More precisely, adversaries can obtain all the smart meter readings by eavesdropping. With curiosity piqued, the adversary will attempt to infer customer's behavior through analyzing the meter readings. But the adversary will not insert, delete or modify those readings, because of the honesty. Furthermore, the adversary is assumed to get α, β, γ, η, $p(i)$, p_{max} and p_{min}.

C. System Goals

Our goal is to design cost-friendly privacy-preserving schemes which can protect the customer's privacy and reduce the cost simultaneously under static and dynamic policies, respectively.

For static policy, the unit electricity price during each time period is announced by the electricity company in advance. In this case, our first goal is defined as Goal 1.

Goal 1: For all i, develop a scheme κ that achieves differential privacy, and $\mathbb{E}(\sum_i (p(i) \times n(i))) \leq 0$, due to α, β, γ, η, C, $c(i-1)$, $\kappa(D_i)$, and $p(i)$.

For dynamic policy, only the maximal and minimal unit electricity prices are publicized, and the electricity company can adjust this unit price autonomously, according to the global energy usage. Therefore, the real-time unit price is uncertain for the customer [16], [17]. In this case, our goal is shown as Goal 2.

Goal 2: For all i, develop a scheme κ that achieves differential privacy, and $\mathbb{E}(\sum_i (p(i) \times n(i))) \leq 0$, due to α, β, γ, η, C, $c(i-1)$, $\kappa(D_i)$, p_{min}, and p_{max}.

V. COST-FRIENDLY DIFFERENTIAL PRIVACY-PRESERVING SCHEMES

In this section, we first design a battery-based differential privacy-preserving (BDP) scheme, when considering the limited charge-discharge rate and capacity of battery. By extending BDP scheme, we further propose two cost-friendly differential privacy-preserving (CDP) schemes under static and dynamic policies, respectively.

A. The Battery-Based Differential Privacy-Preserving Scheme

Since the charge-discharge rate and capacity of the battery are limited ($\gamma \leq n(i) \leq \eta$, $0 \leq c(i) \leq C$), the range of $n(i)$ cannot be drawn from the Laplace distribution, because the domain of Laplace distribution is $(-\infty, +\infty)$, due to Equation (2). Thus, we have to design a new distribution to replace Laplace distribution in smart grid. Formally, the probability density function of the new distribution is presented as follows:

$$pdf(x) = \begin{cases} \frac{e^{-\frac{|x-\mu|}{\sigma}}}{2\sigma T}, & \beta + \gamma - \kappa(D_i) \leq x \leq \alpha + \eta - \kappa(D_i) \\ 0, & \text{Otherwise} \end{cases} \tag{5}$$

where

$$T = \frac{1}{2} e^{-\frac{\beta+\gamma-\kappa(D_i)-\mu}{\sigma}} + \frac{1}{2} e^{\frac{\alpha+\eta-\kappa(D_i)-\mu}{\sigma}} - 1 \tag{6}$$

We prove that $pdf(x)$ is always nonnegative, and its integral from $-\infty$ to ∞ equals 1 in the Appendix. Hence, Equation (5) satisfies the mathematical requirements for the probability density function. In addition, by choosing an appropriate battery, we have $\beta + \gamma < 0$ and $\alpha + \eta > 0$.

Assume that there are M electricity appliances in the house. We now propose the specification of BDP scheme as below.

B. The Cost-Friendly Differential Privacy-Preserving Scheme Under Static Pricing Policy

Since the unit electricity price during each time period is fixed, an intuitive method to save the cost is charge the battery in the lower price and discharge it in the higher price. But this method violates the definition of differential privacy, because the charge-discharge rate has to be stochastic. To settle this problem, we choose to charge the battery with a higher probability for the lower unit price, and discharge the battery with a

Algorithm 1 The Specification of BDP Scheme

```
Input: $\alpha$, $\beta$, $\gamma$, $\eta$, $C$, $c(i-1)$, $\{d_j^i | j \in [1, M]\}$.
Output: $n(i)$.
$\kappa(D_i) = \sum_{j=1}^{M}(d_j^i)$
For all $k, l \in [1, M]$, $\Delta f = \max\left|d_k^i - d_l^i\right|$
$\mu = 0$, $\sigma = \Delta f/\epsilon$
$T = \frac{1}{2}e^{-\frac{\beta+\gamma-\kappa(D_i)-\mu}{\sigma}} + \frac{1}{2}e^{\frac{\alpha+\eta-\kappa(D_i)-\mu}{\sigma}} - 1$
$pdf(x) = \frac{e^{-\frac{|x-\mu|}{\sigma}}}{2\sigma T}$
Do
    $n(i) \leftarrow pdf(x)$
While$(n(i) + c(i-1) > C || n(i) + c(i-1) < 0)$
$c(i) = n(i) + c(i-1)$
Return $n(i)$
```

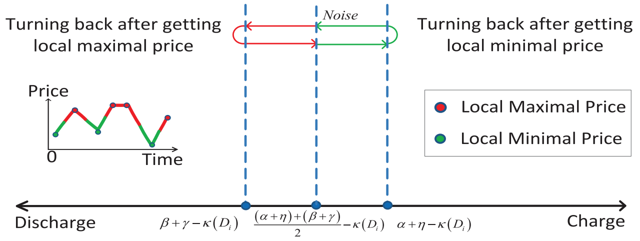
Turning back after getting local maximal price
Noise
Turning back after getting local minimal price
Price
0
Time
Local Maximal Price
Local Minimal Price
Discharge
$\beta+\gamma-\kappa(D_i)$
$\frac{(\alpha+\eta)+(\beta+\gamma)}{2}-\kappa(D_i)$
$\alpha+\eta-\kappa(D_i)$
Charge

Fig. 1. Charge-discharge Rate of Battery under Static Policy.

higher probability for the higher unit price. More specifically, in order to charge battery with higher probability, μ is moved towards $\alpha + \eta - \kappa(D_i)$, till the price reaches a local minimal price $p(t_l)$. Similarly, μ is moved towards $\beta + \gamma - \kappa(D_i)$ to discharge battery with higher probability, till the price arrives at a local maximal price $p(t_h)$, as shown in Figure 1. Besides cost, privacy has also to be considered under static pricing policy. The parameter μ of Laplace distribution is best equal to 0, in order to preserve privacy [21], [22]. Therefore, we assume that the weight of cost is set to w, $(0 \leq w \leq 1)$. Then we have

$$\mu = w \cdot \left((p(i) - p(t_l)) \cdot \frac{(\beta+\gamma) - (\alpha+\eta)}{p(t_h) - p(t_l)} + \alpha + \eta - \kappa(D_i)\right) \tag{7}$$

Assume there are M appliances. We design the cost-friendly differential privacy-protection scheme under static pricing policy (CDP1 scheme, for short). The specification of CDP1 scheme is shown in Algorithm 2.

Algorithm 2 The Specification of CDP1 Scheme

```
Input:$\alpha$, $\beta$, $\gamma$, $\eta$, $C$, $c(i-1)$, $\{d_j^i | j \in [1, M]\}$, $\{p(i)\}$.
Output: $n(i)$.
$\kappa(D_i) = \sum_{j=1}^{M}(d_j^i)$
For all $k, l \in [1, M]$, $\Delta f = \max\left|d_k^i - d_l^i\right|$
If$(p(i) > p(i+1))$
    $tmp_1 = tmp_2 = i$
    While$(p(tmp_1) > p(tmp_1 + 1))\{++tmp_1\}$
    $p(t_l) = p(tmp_1)$
    While$(p(tmp_2) <= p(tmp_2 - 1))\{--tmp_2\}$
    $p(t_h) = p(tmp_2)$
Else If$(p(i) <= p(i+1))$
    $tmp_1 = tmp_2 = i$
    While$(p(tmp_1) < p(tmp_1 + 1))\{++tmp_1\}$
    $p(t_h) = p(tmp_1)$
    While$(p(tmp_2) >= p(tmp_2 - 1))\{--tmp_2\}$
    $p(t_l) = p(tmp_2)$
$\mu = w \cdot ((p(i) - p(t_l)) \cdot \frac{(\beta+\gamma)-(\alpha+\eta)}{p(t_h)-p(t_l)} + \alpha + \eta - \kappa(D_i))$
$\sigma = \Delta f/\epsilon$
$T = \frac{1}{2}e^{-\frac{\beta+\gamma-\kappa(D_i)-\mu}{\sigma}} + \frac{1}{2}e^{\frac{\alpha+\eta-\kappa(D_i)-\mu}{\sigma}} - 1$
$pdf(x) = \frac{e^{-\frac{|x-\mu|}{\sigma}}}{2\sigma T}$
Do
    $n(i) \leftarrow pdf(x)$
While$(n(i) + c(i-1) > C || n(i) + c(i-1) < 0)$
$c(i) = n(i) + c(i-1)$
Return $n(i)$
```

C. The Cost-Friendly Differential Privacy-Preserving Scheme Under Dynamic Pricing Policy

The real-time unit electricity price is uncertain to the customer under dynamic pricing policy [16], [17]. Hence, Equation (7) cannot be used to save the cost any more. Since the customer cannot predict whether the unit price during the next time period will be higher or lower than the current unit price, we cannot decide to charge or discharge the battery for saving the cost. Here we apply the regret mechanism from MAB problem to settle this problem. To attain our goals, privacy preserving and cost saving can be regarded as two kinds of profits. From the point of privacy preserving, the optimal strategy is to set $\mu = 0$, because δ is 0 [22]. The privacy loss is the smallest in this case. From the point of cost saving, greedy strategy has to be used as the price cannot be predicted. Following this strategy, μ chooses the maximal discharge rate from all the possible arms. Then we set a weight w, $(w \in [0, 1])$ to balance the privacy preserving and cost saving. Finally, the regret $\mathcal{R}_n$ is shown as $\mathcal{R}_n = w \cdot |Arm_j| + (1 - w) \cdot (Arm_j - Arm_0)$. Here Arm_j represents the j^{th} arm, and Arm_0 is the arm that has the maximal possible discharge rate.

Assume that all the charge-discharge rates are divided into m parts, and there are M appliances. We design the cost-friendly differential privacy-protection scheme under dynamic policy (CDP2 scheme, for short), as shown in Algorithm 3.

VI. Theoretical Analysis

In this section, we prove the BDP scheme achieves differential privacy, and prove both CDP1 and CDP2 schemes achieve differential privacy and save the cost simultaneously.

A. Privacy Analysis

Theorem 1: BDP scheme achieves differential privacy.

Proof: The proof contains two steps. The first step is to prove the BDP scheme achieves (ϵ, δ) differential privacy at time i, when $-\gamma \leq c(i) \leq (C - \eta)$. In this case, the energy left in the battery $c(i)$ must meet the requirement of all the

Algorithm 3 The Specification of CDP2 Scheme

```
Input: $\alpha,\ \beta,\ \gamma,\ \eta,\ C,\ c(i-1),\ \{d_j^i | j \in [1, M]\},\ p_{min}, p_{max}$
Output: $n(i)$.
1. $\kappa(D_i) = \sum_{j=1}^{M}(d_j^i)$
2. For all $k, l \le M,\ \Delta f = \max\left|d_k^i - d_l^i\right|$
3. For all $j \le m$
4.         $Arm_j = \beta + \gamma - \kappa(D_i) + \frac{j(\alpha+\eta-\beta-\gamma)}{m}$
5.         $\Pr[Arm_j] = 1/m,\ \mathcal{R}_j = 0$
6. $Arm_i \leftarrow \{\Pr[Arm_i] | i \in [1, m]\}$
7. $\mu = Arm_i,\ \sigma = \Delta f/\epsilon$
8. $T = \frac{1}{2}e^{-\frac{\beta+\gamma-\kappa(D_i)-\mu}{\sigma}} + \frac{1}{2}e^{\frac{\alpha+\eta-\kappa(D_i)-\mu}{\sigma}} - 1$
9. $pdf(x) = \frac{e^{-\frac{|x-\mu|}{\sigma}}}{2\sigma T}$
10. Do
11.         $n(i) \leftarrow pdf(x)$
12.While$(n(i) + c(i-1) > C || n(i) + c(i-1) < 0)$
13. $c(i) = n(i) + c(i-1)$
14. $\mathcal{R}_i = w|Arm_i| + (1-w)|Arm_i - Arm_0|$
15. $TR = \sum_{j=1}^{m}(\mathcal{R}_j)$
16. For all $j \le m$, $\Pr[Arm_j] = (TR - \mathcal{R}_j)/TR$
17. Return $n(i)$
```

possible charge/discharge rates, because $\gamma \le n(i) \le \eta$. Then we prove the probability of $c(i) < -\gamma$ or $c(i) > (C - \eta)$ is bounded for all i.

Step 1: For $-\gamma \le c(i) \le (C - \eta)$:

Assume that D_i and D_i' consist of all appliances where only one appliance is different. Since $o(i) = \kappa(D_i) + n(i)$, we have

$$\frac{\Pr[o(i) = \kappa(D_i) + n(i)]}{\Pr\left[o(i) = \kappa\left(D_i'\right) + n'(i)\right]} = \lim_{\Delta x \to 0} \frac{\int_{o(i)-\kappa(D_i)}^{o(i)-\kappa(D_i)+\Delta x} \frac{e^{-\frac{|x-\mu_1|}{\sigma}}}{2\sigma T_1} dx}{\int_{o(i)-\kappa\left(D_i'\right)}^{o(i)-\kappa\left(D_i'\right)+\Delta x} \frac{e^{-\frac{|x-\mu_2|}{\sigma}}}{2\sigma T_2} dx},$$

where

$$T_1 = \frac{1}{2}e^{-\frac{\beta+\gamma-\kappa(D_i)-\mu_1}{\sigma}} - \frac{1}{2}e^{\frac{\alpha+\eta-\kappa(D_i)-\mu_1}{\sigma}} - 1$$
$$T_2 = \frac{1}{2}e^{-\frac{\beta+\gamma-\kappa(D_i)-\mu_2}{\sigma}} - \frac{1}{2}e^{\frac{\alpha+\eta-\kappa(D_i)-\mu_2}{\sigma}} - 1$$

Here $\mu_l \le \mu_1 = \mu_2 = 0 \le \mu_u$, and μ_l is the minimum of all the possible μ. μ_u is the maximum of all the μ. $\Delta f = \max|d_k^i - d_l^i|$ for all the possible k, l and i, $\sigma = \Delta f/\epsilon$, and $T_1, T_2 > 0$. Since $\Delta\mu = |\mu_1 - \mu_2| = 0 \le |\mu_l - \mu_h|$, we have

$$\lim_{\Delta x \to 0} \frac{\int_{o(i)-\kappa(D_i)}^{o(i)-\kappa(D_i)+\Delta x} \frac{e^{-\frac{|x-\mu_1|}{\sigma}}}{2\sigma T_1} dx}{\int_{o(i)-\kappa\left(D_i'\right)}^{o-\kappa\left(D_i'\right)+\Delta x} \frac{e^{-\frac{|x-\mu_2|}{\sigma}}}{2\sigma T_2} dx} = \frac{\frac{e^{-\frac{|o-\kappa(D_i)-\mu_1|}{\sigma}}}{2\sigma T_1}}{\frac{e^{-\frac{\left|o-\kappa\left(D_i'\right)-\mu_2\right|}{\sigma}}}{2\sigma T_2}}$$
$$= \frac{T_2}{T_1}e^{\frac{\left|\kappa\left(D_i'\right)-\kappa(D_i)+\mu_2-\mu_1\right|}{\sigma}} \le \frac{T_2}{T_1}e^{\frac{\left|\kappa\left(D_i'\right)-\kappa(D_i)\right|+|\mu_2-\mu_1|}{\sigma}}$$
$$\le \frac{T_2}{T_1}e^{\epsilon}e^{\Delta\mu} \le \frac{\frac{1}{2}e^{-\frac{\beta+\gamma-\eta-\mu_u}{\sigma}} + \frac{1}{2}e^{\frac{\alpha+\eta-\gamma-\mu_l}{\sigma}} - 1}{\frac{1}{2}e^{-\frac{\beta-\mu_l}{\sigma}} + \frac{1}{2}e^{\frac{\alpha-\mu_u}{\sigma}} - 1}e^{\epsilon}e^{\Delta\mu}$$

Since

$$\frac{\frac{1}{2}e^{-\frac{\beta+\gamma-\eta-\mu_u}{\sigma}} + \frac{1}{2}e^{\frac{\alpha+\eta-\gamma-\mu_l}{\sigma}} - 1}{\frac{1}{2}e^{-\frac{\beta-\mu_l}{\sigma}} + \frac{1}{2}e^{\frac{\alpha-\mu_u}{\sigma}} - 1}e^{\epsilon}e^{\Delta\mu}$$
$$= e^{\epsilon} + e^{\epsilon}\left(\frac{\frac{1}{2}e^{-\frac{\beta+\gamma-\eta-\mu_u}{\sigma}} + \frac{1}{2}e^{\frac{\alpha+\eta-\gamma-\mu_l}{\sigma}} - 1}{\frac{1}{2}e^{-\frac{\beta-\mu_l}{\sigma}} + \frac{1}{2}e^{\frac{\alpha-\mu_u}{\sigma}} - 1}e^{\Delta\mu} - 1\right)$$

we assume that $\delta = \phi \Pr[o(i) = \kappa(D_i') + n'(i)]$, where

$$\phi = e^{\epsilon}\left(\frac{\frac{1}{2}e^{-\frac{\beta+\gamma-\eta-\mu_u}{\sigma}} + \frac{1}{2}e^{\frac{\alpha+\eta-\gamma-\mu_l}{\sigma}} - 1}{\frac{1}{2}e^{-\frac{\beta-\mu_l}{\sigma}} + \frac{1}{2}e^{\frac{\alpha-\mu_u}{\sigma}} - 1}e^{\Delta\mu} - 1\right) \quad (8)$$

We have $\Pr[o(i) = \kappa(D_i) + n(i)] = e^{\epsilon}\Pr[o(i) = \kappa(D_i') + n'(i)] + \delta$.

Therefore, (ϵ, δ) differential privacy is achieved in this case.

Step 2: For all i, we show that the probability of $c(i) < -\gamma$ or $c(i) > (C - \eta)$ is bounded.

(1) For the probability of $c(i) < -\gamma$:

Since $n(i) = c(i) - c(i-1)$ and $0 \le c(i-1) \le C$, we have $\Pr[c(i) < -\gamma] = \Pr[n(i) < -c(i-1) - \gamma] \le \Pr[n(i) - \mathbb{E}(n(i)) < -\gamma - \mathbb{E}(n(i))] \le \frac{\mathbb{D}(n(i))}{[\gamma+\mathbb{E}(n(i))]^2}$

(2) For the probability of $c(i) > (C - \eta)$:

$\Pr[c(i) > (\alpha + \eta)] \le \Pr[n(i) > -C + (C - \eta)] = \Pr[n(i) - \mathbb{E}(n(i)) > -\eta - \mathbb{E}(n(i))] \le \frac{\mathbb{D}(n(i))}{[\eta+\mathbb{E}(n(i))]^2}$

We set $\lambda = \frac{\mathbb{D}(n(i))}{[\gamma+\mathbb{E}(n(i))]^2} + \frac{\mathbb{D}(n(i))}{[\eta+\mathbb{E}(n(i))]^2}$

In the Appendix, we prove that $\mathbb{E}(n(i))$ and $\mathbb{D}(n(i))$ are two fixed numbers, given σ, μ, α, β, γ, η and $\kappa(D_i)$.

In sum, we have

$$\Pr[o(i) = \kappa(D_i) + n(i)] = (1-\lambda)\Pr[o(i) = \kappa(D_i) + n(i)]$$
$$+ \lambda\Pr[o(i) = \kappa(D_i) + n(i)]$$
$$\le (1-\lambda) * \left(e^{\epsilon}\Pr\left[o(i) = \kappa(D_i') + n'(i)\right] + \delta\right) + \lambda * 1$$
$$\le e^{\epsilon}\Pr\left[o(i) = \kappa\left(D_i'\right) + n'(i)\right] + (\delta + \lambda)$$

Therefore, $(\epsilon, \delta + \lambda)$ differential privacy is achieved in this case. ■

We next prove both CDP schemes achieve differential privacy.

Theorem 2: CDP1 and CDP2 schemes achieve differential privacy.

Proof: The only difference between CDP1/CDP2 scheme and BDP scheme is the selection of μ. Owing to the Equation (7), $\Delta\mu$ is always bounded in CDP1 and CDP2 schemes, because $\kappa(D_i)$ is bounded. Consequently, the proof for BDP scheme is also valid for the CDP1 and CDP2 schemes as well. ■

B. Cost Saving Analysis

We first prove CDP1 scheme saves the cost in this section.

Theorem 3: Given α, β, γ, η, C, $c(i-1)$, $\kappa(D_i)$, and $\{p(i)\}$ CDP1 scheme satisfies $\mathbb{E}(\sum_i(p(i) \times n(i))) \le 0$ for all i.

Proof: Since $\beta+\gamma < 0$ and $\kappa(D_i) \ge 0$, we have $\mathbb{E}(\sum_i(p(i) \times n(i))) \le \sum_i\{p(i) \cdot w \cdot ((p(t_h) - p(t_l)) \cdot \frac{(\beta+\gamma)-(\alpha+\eta)}{p(t_h)-p(t_l)} + \alpha + \eta - \kappa(D_i))\} = \sum_i\{p(i) \cdot w \cdot (\alpha + \eta - \kappa(D_i))\} \le 0$. ■

TABLE II
DEFAULT VALUE OF ALL THE PARAMETERS

Δt	0.25 Hours	ϵ	0.1
η	8 kW	γ	-8 kW
α	6.081 kWh	β	0 kWh
C	4 kWh	$c(0)$	0 kWh
w	0.5	m	100 (Arms)
p_{max}	0.02109 \$/kWh	p_{min}	0.00704 \$/kWh

We then indicate that CDP2 scheme also saves the cost. Note that which arm is chosen does not rely on the price, because $\mathcal{R}_i$ is independent with $p(i)$, for all i.

Theorem 4: Given α, β, γ, η, C, $c(i-1)$, $\kappa(D_i)$, p_{min} and p_{max}, CDP2 scheme satisfies $\mathbb{E}(\sum_t(p(i)\times n(i)))\leq 0$ for all i.

Proof: The math expectation of cost is $\mathbb{E}(\sum_i(p(i)\times n(i))) = \mathbb{E}(\sum_i(p(i)\cdot\sum_{j=1}^{m}((1-\mathcal{R}_j/TR)\cdot Arm_j)) \leq \mathbb{E}(\sum_i(p(i)\cdot Arm_j)) = \mathbb{E}(\sum_i p(i))\cdot\mathbb{E}(Arm_j)$.

For $Arm_j\geq 0$, $\mathcal{R}_j = w|Arm_j| + (1-w)(Arm_j - Arm_0) = (Arm_j - Arm_0) + w\cdot Arm_0$, so $\mathcal{R}_j$ is the minimum when $Arm_j = 0$. Additionally, for $Arm_i < 0$, $\mathcal{R}_j = (Arm_j - Arm_0) - w\cdot(2\cdot Arm_j - Arm_0)$, thus $\mathcal{R}_j$ is the minimum when $Arm_j = Arm_0 \leq 0$. Since the probability to choose Arm_j is based on $\mathcal{R}_i$ and $\mathbb{E}(Arm_j)\leq 0$, we have $\mathbb{E}(\sum_i(p(i)\times n(i)))\leq 0$. ■

VII. EXPERIMENTAL ANALYSIS

Although differential privacy maintains the privacy loss at about the same level, we still need to quantitatively evaluate the total privacy loss. Therefore, we first apply the traditional mutual information metric to compare the global privacy leakage of CDP1 and CDP2 schemes with MBE, PRIVATUS and OPPEM schemes in this section. Since CDP1 and CDP2 scheme achieves differential privacy, we then show the relationship between ϵ and δ for CDP1 and CDP2 scheme. We next compare the cost saving for CDP1 and CDP2 schemes under different pricing policies. Finally, we also compare the cost saving for different weights of cost in CDP1 and CDP2 schemes.

We first compare the global privacy loss of CDP1 and CDP2 schemes with MBE, PRIVATUS, OPPEM schemes. To show the stability of both CDP schemes, multiple experiments are conducted with different capacities of battery and different TOU pricing policies. Here, we use the dataset REDD [25] from MIT. We extract the average electricity consumption at the interval of 15 minutes for three different houses as the customer's electric consumption information. The minimum power that the adversary can distinguish is assumed to be 0.001 kW. The lowest and highest price is from Salt River Project TOU price plans [16]. The default values of all the parameters are specified in Table II.

Since all the delta values of two adjacent meter readings and all the values of meter readings are both useful to the adversaries [13], we define two kinds of mutual information MI_0 and MI_1 as follows. Assume that $\kappa'(D_i) = \kappa(D_i) - \kappa(D_{i-1})$, and $o'(i) = o(i) - o(i-1)$, we have

$$MI_0 = \sum_i\sum_{\kappa'(i)}\sum_{o'(i)}\Pr\big(\kappa'(i), o'(i)\big)\log\frac{\Pr\big(\kappa'(i), o'(i)\big)}{\Pr(\kappa'(i)\cdot\Pr(o'(i)))} \tag{9}$$

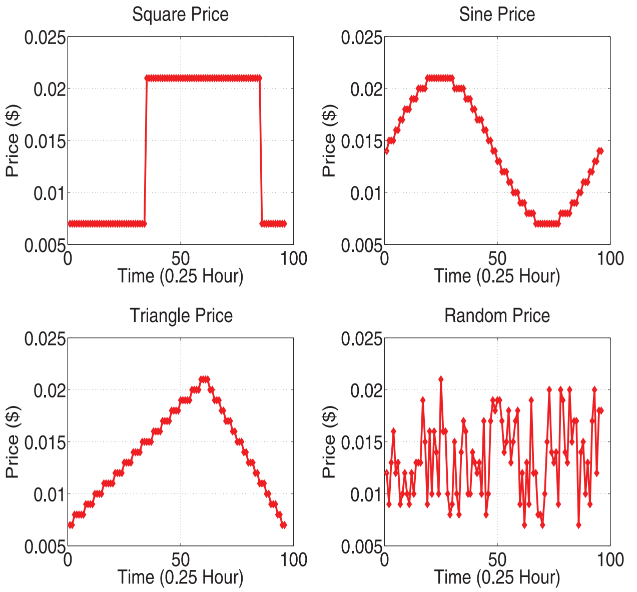

Fig. 2. Different pricing policies.

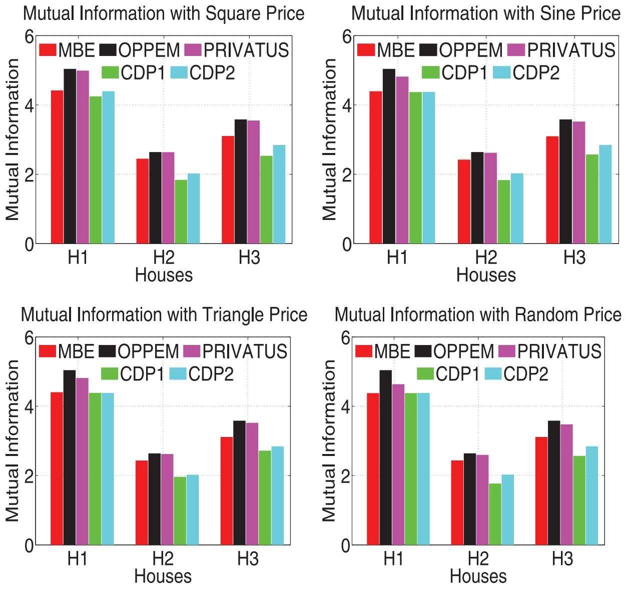

Fig. 3. Maximal privacy loss in three houses.

$$MI_1 = \sum_i\sum_{\kappa(i)}\sum_{o(i)}\Pr(\kappa(i), o(i))\log\frac{\Pr(\kappa(i), o(i))}{\Pr(\kappa(i)\cdot\Pr(o(i)))} \tag{10}$$

Fifty experiments are run to compute the average for all the schemes. Figure 2 shows four pricing policies (square, sine, triangle and random). The first three pricing policies belong to static policy, while the random pricing policy simulates the dynamic policy. For each policy, there are 24/0.25 = 96 unit prices in a day.

Figure 3 shows maximal privacy loss for all the schemes in three different houses, respectively. The smaller MI_0 and MI_1 are, the less the privacy loss is. Moreover, we choose the higher value between MI_0 and MI_1 as the final privacy loss. From the results, we can see that the privacy loss of CDP1 and CDP2 schemes are no bigger than that of the other three schemes.

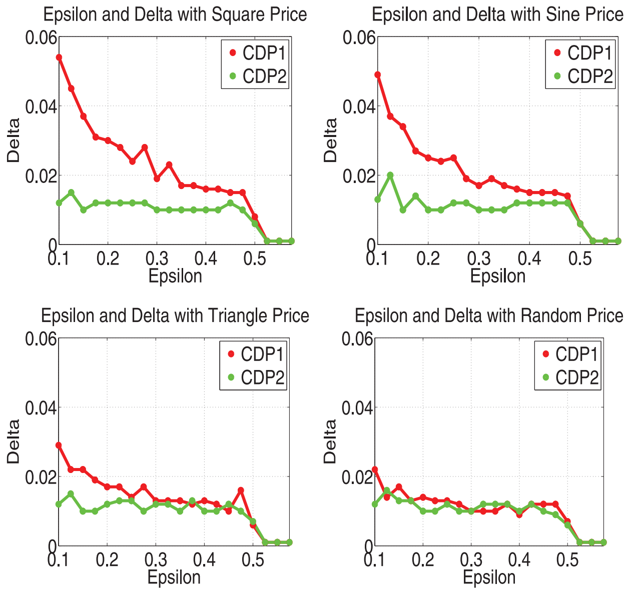

Fig. 4. The relationship between δ and ϵ in the house 1.

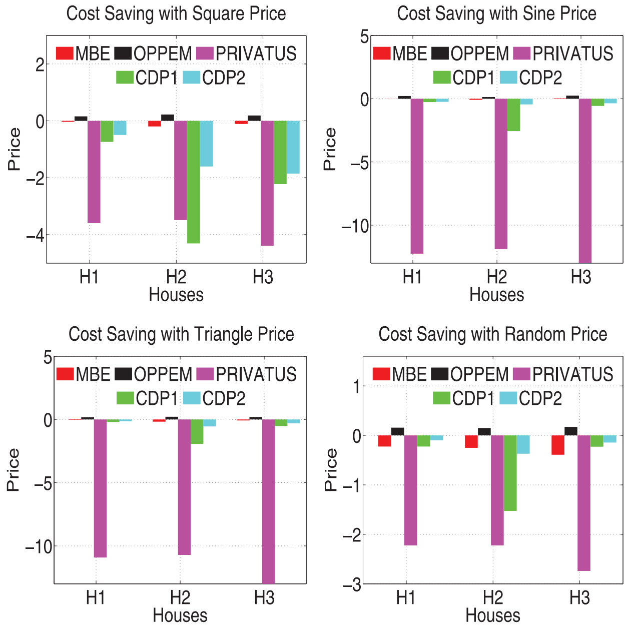

Fig. 5. Maximal cost saving in three houses.

We then show the relationship between δ and ϵ for CDP1 and CDP2 schemes in Figure 4. We can see that the larger ϵ is, the smaller δ is. Besides, the value of δ is always less than 0.1 in our schemes. This guarantees that the privacy is protected about the same level in our experiments.

Next, we compare the cost saving of CDP1 and CDP2 schemes with MBE, PRIVATUS and OPPEM schemes. The parameters are the same as that in Table II. A negative value indicates that the customer earns money by charging or discharging the battery. From Figure 5, both CDP1 and CDP2 schemes truly save the cost during in all the experiments.

Finally, the customer's cost saving is compared under different weights for both CDP1 and CDP2 schemes. Specifically, the weight of cost changes from 0 to 1, as shown in Figure 6.

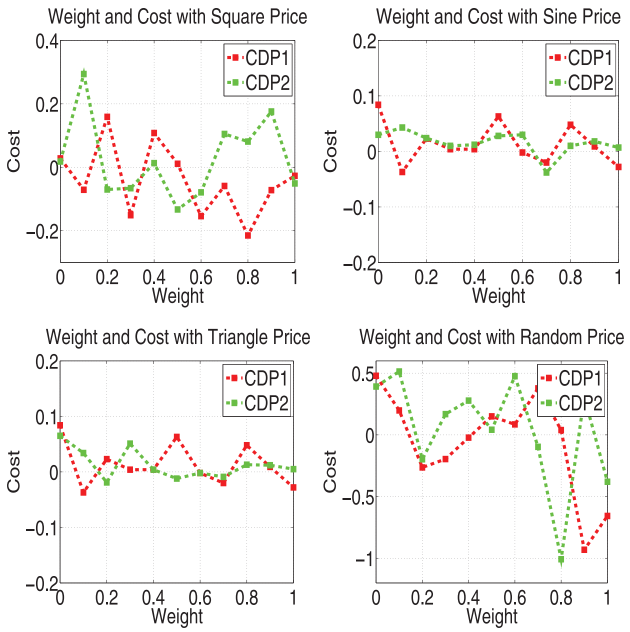

Fig. 6. The weight of cost in the house 1.

The trend of cost goes down under all the pricing policies, with the increasing of the weight. This represents that the customer will save more money if the weight of cost increases.

VIII. Conclusion

In this paper, we introduced two cost-friendly differential privacy-preserving schemes under static and dynamic time-of-use pricing policies. Theoretical analysis proved that both schemes attained the goals of preserving privacy and saving cost simultaneously, when the limited capacity and charge-discharge rate of the battery was considered. Experimental analysis showed that the privacy loss for both CDP1 and CDP2 schemes were smaller than that for the existing schemes. Additionally, our schemes supports both static and dynamic pricing policies. Future efforts will focus on investigating the battery's capacity loss and customer's electricity usage habit, in order to precisely depict the battery and reduce more cost. Besides, more strategies, such as epsilon-greedy or epsilon-decreasing strategy, of solving multiple-armed bandit problem [23], [24] will be tried to decrease privacy leakage.

Appendix

We first show that $pdf(x)$ is a valid probability density function here. Since $T \geq 0$, we have $pdf(x) \geq 0$. In addition,

$$F(x) = \int_{-\infty}^{+\infty} f(x)dx = \int_{\beta+\gamma-\kappa(D_i)}^{\alpha+\eta-\kappa(D_i)} \frac{e^{-\frac{|x-\mu|}{\sigma}}}{2\sigma T} dx = \frac{T}{T} = 1$$

Next, we compute the expected value $\mathbb{E}(x)$ of the probability distribution, given σ, μ, α, β, γ, η and $\kappa(D_i)$.

$$\begin{aligned}\mathbb{E}(x) &= \int_{-\infty}^{+\infty} xf(x)dx = \int_{\beta+\gamma-\kappa(D_i)}^{\alpha+\eta-\kappa(D_i)} xf(x)dx \\ &= \int_{\beta+\gamma-\kappa(D_i)}^{\mu} \frac{x}{2\sigma T} e^{\frac{x-\mu}{\sigma}} dx + \int_{\mu}^{\alpha+\eta-\kappa(D_i)} \frac{x}{2\sigma T} e^{\frac{\mu-x}{\sigma}} dx\end{aligned}$$

$$= \frac{\sigma e^{-\frac{\mu}{\sigma}}}{2T}(x-1)e^x \Big|_{\frac{\beta+\gamma-\kappa(D_i)}{\sigma}}^{\frac{\mu}{\sigma}} + \frac{\sigma e^{\frac{\mu}{\sigma}}}{2T}(x-1)e^x \Big|_{-\frac{\mu}{\sigma}}^{-\frac{\alpha+\eta-\kappa(D_i)}{\sigma}}$$

Assume $L = \alpha + \eta - \kappa(D_i)$ and $H = \beta + \gamma - \kappa(D_i)$. Given σ, μ,α, β, γ, η and $\kappa(D_i)$, and $\mathbb{E}(x)$, the variance $\mathbb{D}(x)$ is computed as follows:

$$\begin{aligned}\mathbb{D}(x) &= \int_{-\infty}^{+\infty}(x-\mathbb{E}(x))^2 f(x)dx = \int_{H}^{L}(x-\mathbb{E}(x))^2 f(x)dx \\ &= \frac{\sigma^2 e^{-\frac{\mu}{\sigma}}}{2T}\Big(x^2-2x+2\Big)e^x\Big|_{\frac{\,}{\sigma}}^{\frac{\mu}{\sigma}} - \mathbb{E}(x)e^{-\frac{\mu}{\sigma}}(x-1)e^x\Big|_{\frac{H}{\sigma}}^{\frac{\mu}{\sigma}} \\ &\quad + \frac{\mathbb{E}^2(x)e^{-\frac{\mu}{\sigma}}}{2T}e^x\Big|_{\frac{H}{\sigma}}^{\frac{\mu}{\sigma}} - \frac{\sigma^2 e^{\frac{\mu}{\sigma}}}{2T}\Big(x^2-2x+2\Big)e^x\Big|_{-\frac{\mu}{\sigma}}^{-\frac{L}{\sigma}} \\ &\quad - \mathbb{E}(x)e^{-\frac{\mu}{\sigma}}(x-1)e^x\Big|_{-\frac{\mu}{\sigma}}^{-\frac{L}{\sigma}} - \frac{\mathbb{E}^2(x)e^{-\frac{\mu}{\sigma}}}{2T}e^x\Big|_{-\frac{\mu}{\sigma}}^{-\frac{L}{\sigma}}.\end{aligned}$$

REFERENCES

[1] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 944–980, 4th Quart. 2012.

[2] E. Commission. (2014). *Cost-Benefit Analyses and State of Play of Smart Metering Deployment in the EU-27*. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014SC0189

[3] K. Ehrhardt-Martinez, K. A. Donnelly, and J. A. Laitner, *Advanced Metering Initiatives and Residential Feedback Programs: A Meta-Review of Household Electricity-Saving Opportunities*. Washington, DC, USA: Amer. Council Energy Efficient Economy, 2010.

[4] H. Farhangi, "The path of the smart grid," *IEEE Power Energy Mag.*, vol. 8, no. 1, pp. 18–28, Jan./Feb. 2010.

[5] S. Darby, "The effectiveness of feedback on energy consumption," Working Paper, Environ. Change Inst., Univ. Oxford, Oxford, U.K., 2006.

[6] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77, May/Jun. 2009.

[7] M. Zeifman and K. Roth, "Nonintrusive appliance load monitoring: Review and outlook," *IEEE Trans. Consum. Electron.*, vol. 57, no. 1, pp. 76–84, Feb. 2011.

[8] D. J. Hess and J. S. Coley, "Wireless smart meters and public acceptance: The environment, limited choices, and precautionary politics," *Public Understand. Sci.*, vol. 23, no. 6, pp. 688–702, 2014.

[9] S. R. Rajagopalan, L. Sankar, S. Mohajert, and H. V. Poor, "Smart meter privacy: A utility-privacy framework," in *Proc. 2nd IEEE Int. Conf. Smart Grid Commun.*, Brussels, Belgium, 2011, pp. 190–195.

[10] G. Kalogridis, C. Efthymious, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Gaithersburg, MD, USA, 2010, pp. 232–237.

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

[12] W. Yang *et al.*, "Minimizing private data disclosures in the smart grid," in *Proc. 16th ACM Conf. Comput. Commun. Security*, 2012, pp. 415–427.

[13] J. Zhao, T. Jung, Y. Wang, and X. Li, "Achieving differential privacy of data disclosure in the smart grid," in *Proc. 33rd IEEE Conf. Comput. Commun.*, Toronto, ON, Canada, 2014, pp. 504–512.

[14] M. Backes and S. Meiser, "Differentially private smart metering with battery recharging," in *Proc. Data Privacy Manag. Auton. Spontaneous Security*, 2014, pp. 194–212.

[15] K. Jessoe, D. Rapson, and J. B. Smith, "The effect of a mandatory time-of-use pricing reform on residential electricity use," in *Proc. Amer. Econ. Assoc. Annu. Meeting*, 2013, pp. 1–54.

[16] L. Yang, X. Chen, J. Zhang, and H. V. Poor, "Optimal privacy-preserving energy management for smart meters," in *Proc. 33rd IEEE Conf. Comput. Commun.*, Toronto, ON, Canada, 2011, pp. 513–521.

[17] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, "UDP: Usage-based dynamic pricing with privacy preservation for smart grid," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 141–150, Mar. 2013.

[18] J. Koo, X. Lin, and S. Bagchi, "PRIVATUS: Wallet-friendly privacy protection for smart meters," in *Proc. 17th Eur. Symp. Res. Comput. Security*, Pisa, Italy, 2012, pp. 343–360.

[19] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 2008.

[20] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York, NY, USA: Wiley, 1991.

[21] C. Dwork and J. Lei, "Differential privacy and robust statistics," in *Proc. 41st Annu. ACM Symp. Theory Comput.*, Bethesda, MD, USA, 2009, pp. 371–380.

[22] C. Dwork, "Differential privacy," in *Proc. 33rd Int. Conf. Autom. Lang. Program. Volume Part II (ICALP)*, Venice, Italy, 2006, pp. 1–12.

[23] P. Auer, N. Cesa-Bianchi, Y. Freund, and R. E. Schapire, "Gambling in a rigged casino: The adversarial multi-armed bandit problem," in *Proc. 36th Annu. Symp. Found. Comput. Sci.*, Milwaukee, WI, USA, 1995, pp. 322–331.

[24] S. Bubeck and N. Cesa-Bianchi, "Regret analysis of stochastic and nonstochastic multi-armed bandit problems," *Found. Trends Mach. Learn.*, vol. 5, no. 1, pp. 1–122, 2012.

[25] J. Z. Kolter and M. J. Johnson, "REDD: A public data set for energy disaggregation research," in *Proc. SustKDD Workshop Data Min. Appl. Sustain.*, San Diego, CA, USA, 2011, pp. 59–62.

Zijian Zhang is an Assistant Professor with the Department of Computer Science, Beijing Institute of Technology. He was a Visiting Scholar with the Computer Science and Engineering Department, State University of New York at Buffalo, in 2015. His research interests include smart grid, data privacy, and mobile security.

Zhan Qin is currently pursuing the Ph.D. degree with the Ubiquitous Security and Privacy Research Laboratory, Computer Science and Engineering Department, State University of New York at Buffalo, NY, USA. His current research interests focus on data privacy, crowdsourcing security, and smart grid.

Liehuang Zhu is a Professor with the Department of Computer Science, Beijing Institute of Technology. He was selected into the Program for New Century Excellent Talents with the University from Ministry of Education, China. His research interests include Internet of Things, cloud computing security, and Internet and mobile security.

Jian Weng is a Professor with the College of Information Science and Technology, Jinan University. He was selected into the Program for New Century Excellent Talents with the University from Ministry of Education, China. His research interests include cryptography and information security.

Kui Ren is a Professor and the Director of the Ubiquitous Security and Privacy Research Laboratory, Computer Science and Engineering Department, State University of New York at Buffalo. His current research interests focus on data and computation outsourcing security in the context of cloud computing, wireless systems security inspired by physical-layer properties, and crowdsourcing-based large-scale information infrastructure building.