UDP: Usage-based Dynamic Pricing with Privacy Preservation for Smart Grid

Xiaohui Liang, *Student Member, IEEE*, Xu Li, Rongxing Lu, *Member, IEEE*,
Xiaodong Lin, *Member, IEEE*, and Xuemin (Sherman) Shen, *Fellow, IEEE*

***Abstract*—Smart sensing and wireless communication technologies enable the electric power grid system to deliver electricity more efficiently through the dynamic analysis of the electricity demand and supply. The current solution is to extend the traditional static electricity pricing strategy to a time-based one where peak-time prices are defined to influence electricity usage behavior of customers. However, the time-based pricing strategy is not truly dynamic and the electricity resource cannot be optimally utilized in real time. In this paper, we propose a usage-based dynamic pricing (UDP) scheme for smart grid in a community environment, which enables the electricity price to correspond to the electricity usage in real time. In the UDP scheme, to simplify price management and reduce communication overhead, we introduce distributed community gateways as proxies of the utility company to timely respond to the price enquiries from the community customers. We consider both community-wide electricity usage and individual electricity usage as factors into price management: a customer gets higher electricity unit price if its own electricity usage becomes larger under certain conditions of the community-wide collective electricity usage. Additionally, we protect the privacy of the customers by restricting the disclosure of the individual electricity usage to the community gateways. Lastly, we provide privacy and performance analysis to demonstrate that the UDP scheme supports real-time dynamic pricing in an efficient and privacy-preserving manner.**

***Index Terms*—Smart grid; dynamic price; privacy preservation; community-specific**

I. Introduction

Smart grid has emerged as the next-generation power grid through the convergence of power system engineering and communication technology [1]–[3]. It features millions of intelligent networked electronic equipments, e.g. smart meters, sensors, automatic control devices, deployed in the power grid. The use of these equipments coupled with a dynamic pricing (DP) strategy [4]–[6] enables the power grid to transform from a traditional load-following operating mode to an advanced load-shaping mode, where electricity demands are managed adaptively to meet the electricity generation and distribution capabilities at any time. Traditionally, the power system is scheduled only for resource generation because the majority of power system loads are neither controllable nor measurable at the required time resolution. In addition, the time-independent retail electricity price provides little incentive for customers to schedule their electricity consumption. With the pervasive networked electronic equipments, the smart grid brings customers with an advanced and efficient communication system which can instantly deliver the electricity usage from customers to an electric utility company. Here, an electric utility company means the company that buys and sells electricity, acting as a broker in the electricity market [7]. For simplicity, in the following, we use "utility company" for "electric utility company". In the smart grid, the utility company is able to set dynamic price information for customers corresponding to their electricity usage. The dynamic price information can be timely delivered to the customers, and the customers have more economic incentives to re-schedule their daily electricity usage. With the help of pervasive networked equipments, the DP strategy can eventually shift the electricity demands from peak time to non-peak time, and therefore improve stability and reduces production costs of the power grid in the long run.

The success of the DP strategy highly depends on the customers' actual response to the time-varying prices. However, it is generally inconvenient and impractical for the customers to manually report the usage and track the prices. To overcome this difficulty, intelligent smart meters equipped with an automatic price-aware scheduling mechanism must be trusted and adopted by the customers. Extensive research efforts have been made to develop these mechanisms by exploiting prediction model [8], Markov chain model [4], and game theoretic model [9]. In this paper, we investigate the DP strategy in smart grid from two novel aspects: distributed price management and privacy preservation of individual electricity usage. Distributed price management is a necessity for the future smart grid as the electricity demands and electricity generation/distribution capabilities are distinct according to not only time but also locations. Following the hierarchical network structure of smart grid, we require price management to be carried out within *community networks*. In each community network, there is a community gateway (CG) to communicate with the local customers for the electricity usage collection and the price indication. Such a gateway provides fast response to the price enquiries from the customers and reduces the communication overhead of the utility company. Privacy preservation is another critical component to the success of smart grid deployment, as recognized by many standardization bodies, e.g. National Institute of Standards and Technology (NIST) [10]. Without appropriate and robust privacy policies, the

Manuscript received 31 March 2012; revised 5 September 2012.

X. Liang, R. Lu, and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Canada (emails: {x27liang, rxlu, xshen}@bbcr.uwaterloo.ca).

X. Li is with Huawei Technologies Canada. Part of this work was done when he was with Inria, France (email: easylix@gmail.com).

X. Lin is with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Canada (email: xiaodong.lin@uoit.ca).

customers may be reluctant to get involved in the DP strategy where their electricity usage has to be reported to the CGs all the time. Thus, the DP strategy may not work well as expected. It is worth noting that the security issues of the DP strategy in smart grid are also important, such as device attacks [11] and access control [12]. In this paper, we mainly focus on privacy issues, i.e., protecting individual electricity usage of customers. Our contributions are summarized as follows.

We propose a usage-based dynamic pricing (UDP) scheme with privacy preservation for smart grid in a community environment. The UDP scheme protects the individual customers' electricity usage from disclosure to the CG while enabling the CG to generate the price indication for the customers based on the community-wide electricity usage and the individual electricity usage. We provide an extensive privacy analysis to obtain the exact probability that the CG and the compromised customers correctly guess the electricity usage of a target customer. Furthermore, we improve the UDP scheme to achieve enhanced privacy with reasonable communication cost and computation overhead. We show that the enhanced UDP scheme provides the highest privacy level, i.e., the CG has the smallest probability of having a correct guess on the electricity usage of the target customer.

The remainder of this paper is organized as follows. In Section II, we present the related work. We introduce the network architecture of smart grid and propose a new DP strategy respectively in Sections III and IV. In accordance with the new strategy, we give the detailed constructions in Sections V and VI, along with the privacy analysis presented in Section VII. We further show how to achieve enhanced privacy in Section VIII. Finally, we conclude the paper in Section IX.

II. Related Work

A. Electricity Pricing

To schedule the electricity load, the utility company adopts the conventional direct load control (DLC) strategy [13] where smart switches are installed inside of houses such that the house appliances can be turned off during a high-demand period. The DLC enforces the customers to abandon the control of their appliances at certain conditions. Recently, in Ontario, Canada, a Time-Of-Use (TOU) pricing strategy has been widely adopted by utility companies, e.g., Hydro One [14], Waterloo North Hydro [15]. TOU means that the electricity unit price changes according to the time of the day. The Ontario Energy Board (OEB) divides daily and seasonal TOU periods into three categories: off-peak, mid-peak, and on-peak. TOU enables the customers to view the electricity usage online and potentially influences electricity usage behavior of the customers. Though the period settings of TOU can be updated, TOU is neither truly dynamic nor related to the real-time usage. Therefore, TOU may cause some inappropriate situation. For example, in a pre-defined on-peak period, when total electricity usage is in fact low, the over-supplied electricity cannot be economically stored as electrical energy [16] and the customers should be given more incentive to consume more electricity. However, the high on-peak price discourages the electricity consumption of the customers. As a great benefit of smart grid, the dynamic pricing (DP) strategy ensures enough flexibility for the customers (i.e., without setting an upper bound of usage) and is more friendly to meet their demands. In this paper, we propose a new DP strategy by relating the price to the electricity usage in real time, and therefore the high on-peak price issue is avoided.

B. Security and Privacy in Smart Grid

Security and privacy are critical to the development of real-time DP strategy in smart grid. As the electricity usage information is frequently exchanged between the customers, the CGs, and the utility companies, to prevent the security attacks and the privacy violations is critical. Khurana et al. [17] and Li et al. [18] summarized security, trust, and privacy issues in a comprehensive smart grid system. They presented the security and privacy challenges of smart grid system design such as transmission substations, policy-based data sharing, and attestation for constrained smart meters. Lu et al. [19] proposed an efficient and privacy-preserving aggregation scheme (EPPA) for smart grid communications. The EPPA uses a super-increasing sequence to construct multi-dimensional data, and encrypts the structured data by the homomorphic Paillier cryptosystem technique. For data communications from the customers to the operation center, data aggregation is performed directly on ciphertexts at gateways without decryption, and the aggregation result of the original data can be obtained at the operation center. Acs and Castelluccia [20] exploited the privacy-preserving aggregation technique of time-series data in smart meters. The proposed scheme employs a differential privacy model in which the customers add noise to their electricity usage and the aggregator can successfully obtain the sum of the usage with a very large probability. However, in the smart grid, the sum of the usage of the customers is very critical since it directly influences the electricity price and accordingly the electricity usage behavior of the customers. Thus, the customer electricity usage needs to be frequently and accurately collected. This requirement imposes a large amount of communication overhead on the customers and the utility company. In this paper, we propose a distributed pricing strategy where the CGs distributedly interact with the local customers and ensure the dynamic price information to be delivered in a timely fashion. We regard the CGs as the proxies of the utility company and explore the privacy issues for this scenario.

C. Crypto-technique: Homomorphic Encryption

Homomorphic encryption [21] provides the addition and multiplication operations over ciphertexts; a user is able to process the plaintext without knowing the secret keys. With this property, homomorphic encryption is widely used in data aggregation and computation specifically for privacy-sensitive content [19]. We review the homomorphic encryption scheme in [21] which serves a building block of our proposed UDP scheme.

A central authority runs a generator $\mathcal{G}$ which outputs $\langle p, q, R, R_q, R_p, \chi\rangle$ as system public parameters:

- $p < q$ are two primes s.t. $q \equiv 1 \pmod{p}$ and p;

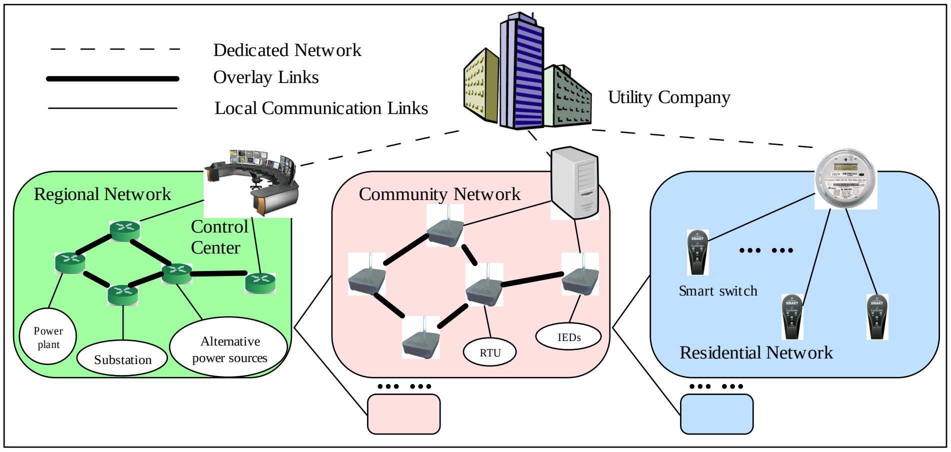


Fig. 1. Network architecture for smart grid

- Rings $R := \mathbb{Z}/\langle x^2+1\rangle$, $R_q := R/qR = \mathbb{Z}_q[x]/\langle x^2+1\rangle$;
- Message space $R_p := \mathbb{Z}_p/\langle x^2+1\rangle$;
- A discrete Gaussian error distribution $\chi = D_{\mathbb{Z}^n,\sigma}$ with standard deviation σ.

Suppose a customer U_i has a public/private key pair (pk_i, sk_i) such that $pk_i = \{a_i, b_i\}$, with $a_i = -(b_i s + pe)$, $b_i \in R_q$ and $s, e \in \chi$, and $sk_i = s$. Let $b_{i,1}$ and $b_{i,2}$ be two messages encrypted by U_i.

- Encryption $E_{pk_i}(b_{i,1})$: $c_{i,1} = (c_0, c_1) = (a_i u_t + p g_t + b_{i,1}, b_i u_t + p f_t)$, where u_t, f_t, g_t are samples from χ.
- Decryption $D_{sk_i}(c_{i,1})$: If denoting $c_{i,1} = (c_0, \cdots, c_\alpha)$, $b_{i,1} = (\sum_{k=0}^{\alpha} c_k s^k) \mod p$.

Consider the two pieces of ciphertext $ct_1 = E(b_{i,1}) = (c_0, \cdots, c_{\alpha_1})$ and $ct_2 = E(b_{i,2}) = (c'_0, \cdots, c'_{\alpha_2})$.

- Addition: Let $\alpha = max(\alpha_1, \alpha_2)$. If $\alpha_1 < \alpha$, let $c_{\alpha_1+1} = \cdots = c_\alpha = 0$; If $\alpha_2 < \alpha$, let $c'_{\alpha_2+1} = \cdots = c'_\alpha = 0$. Thus, we have $E(b_{i,1} + b_{i,2}) = (c_0 \pm c'_0, \cdots, c_\alpha \pm c'_\alpha)$.
- Multiplication: Let v be a symbolic variable and compute $(\sum_{k=0}^{\alpha_1} c_k v^k) \cdot (\sum_{k=0}^{\alpha_2} c'_k v^k) = \hat{c}_{\alpha_1+\alpha_2} v^{\alpha_1+\alpha_2} + \cdots + \hat{c}_1 v + \hat{c}_0$. Thus, we have $E(b_{i,1} \times b_{i,2}) = (\hat{c}_0, \cdots, \hat{c}_{\alpha_1+\alpha_2})$.

III. Smart Grid Network Architecture

Smart grid requires an efficient communication platform for monitoring and controlling the grid operations. By generalizing previous proposals [18], [22], [23], we present a hierarchical network structure of smart grid including three layers, i.e. a residential network layer, a community network layer, and a regional network layer, as illustrated in Fig. 1.

Residential networks are at the bottom layer, each corresponding to a distinct customer. A residential network has a star-like topology, composed of a smart meter at the center and a few control switches (if any exits) at peripheral. As the interface of the network, the smart meter provides real-time raw metering data to the control center at the top layer, and detailed energy usage and price information to the customer. It also accepts control commands from the upper layers to connect/disconnect particular appliances (through pre-installed control switches) for load balancing purposes.

Community networks are at the middle layer. A community network connects to the residential networks, Intelligent Electric Devices (IEDs) and Remote Terminal Units (RTUs) in a neighborhood together. Data storage devices may additionally be included in the network to support networked storage, local fault diagnosis and distributed decision making. There is a communication gateway in each community network. It manages the communication among the network elements, performs data aggregation, and bridges the bottom and top layers to allow data exchange. An example of community network is the network in a smart community [24].

Regional networks are at the top layer. A regional network connects to the community networks, power plants, renewable power sources, substations, feeders and other grid devices in a geographic region. Dedicated hub nodes may be deployed in the network to build a multiple hop overlay structure for efficient and reliable data communication. A control center is implemented in each regional network. It provides SCADA (supervisory control and data acquisition) functionalities in the regional grid: collecting electricity usage and grid operation status, detecting and responding to anomalies, and optimizing power generation, transmission and distribution.

In the above presented architecture, each network is realized by high-speed wired or wireless links or the combination thereof, and runs IP-based communication protocols. Supporting IP allows devices with different physical details to be straightforward integrated and managed in a unified way. Further, control centers, CGs and smart meters could be connected through dedicated networks. With the reliable and efficient connections, the customers may access their own electricity usage and cost information, utility companies may obtain electricity usage information at different granularities, and control centers may share data and coordinate to make inter-regional decisions.

IV. A New Dynamic Pricing Strategy

The objective of the DP strategy is to discourage concentrated electricity usage and flatten peak load in the power system. The price is subject to multiple factors such as location, time, and usage. Current pricing strategy links the price to time and location only and ignores its usage-dependent nature. Within a given time period, the strategy provides indiscriminately treatment to the customers that use electricity differently (in amount, for example) and may have limited and even improper effect on load shifting. For instance, even if only a few customers are consuming electricity during predefined peak time and the total load is far lower than the power system capacity, the price maybe set to a high value and possibly cause unnecessarily reduced electricity usage. Here, we suggest a new DP strategy with consideration of the actual individual electricity usage and the community-wide electricity usage. The strategy is applied at the community network layer of smart grid hierarchy.

Consider a community network composed of n homogenous customers $U_1, \cdots, U_n$ and one CG [24]. Time is slotted. At each time slot t, the electricity usage of a customer U_i is denoted by $e_{i,t}$, and the community-wide electricity usage is given as $e_{s,t} = \sum_{i=1}^{n} e_{i,t}$. The CG obtains a usage threshold e_m from the utility company to differentiate peak time and regular time. If $e_{s,t} \geq e_m$, the time slot t will be regarded as a peak time and the price will be set to a peak-time price; otherwise, it will be a regular time and the price is the regular-time price. Note that, in regular time, the price p_1 will be kept static to all the customers and the customers have enough incentive to use more electricity. In peak-time, the CG calculates $e_a = e_m/n$ as a threshold to differentiate two kinds of customers. For the customers with usage no larger than e_a, the price p_2 is higher than that in regular-time. These customers do not over-consume electricity and their behavior should not be largely influenced. For the customers with usage larger than e_a, the dynamic price p_3 is calculated by using a polynomial function $f()$ with the individual usage $e_{i,t}$ as an input. These customers are regarded as the main contributors of peak time, and the price function $f()$ outputs a higher price than both p_1 and p_2. It also varies among customers. The electricity price setting is shown in Table I. Specifically, according to the studies of power system in [25] and [26], the power-cost relation can be represented by a quadratic polynomial $f(x) = a + bx + cx^2$ where x is the generated power and $f()$ is the total cost. In practice, the utility company defines the coefficients (a, b, c) toward different communities in different regions. The coefficients can be also related to the usage sum $e_{s,t}$ with respect to the given community and time. It is required that $f(e_a) = p_2$ to keep the function with continuity. The utility company can enforce a more complicated price policy.

The responsibility of the CG is to notify the customers of the price information so that the customers are able to adjust their electricity usage and avoid large bills. The CG can be regarded as a proxy authorized by the utility company which initializes the price parameters for the CG. The CG then calculates and sends price information to the customers per each time slot. In this setting, the utility company is not necessarily bothered by the request-and-response process from the customers. At the meantime, the customers receive authentic price information from the CG while the individual electricity usage will not be revealed to the CG. In the UDP scheme, the customers set price threshold values and implicitly send them to the CG which will then reply whether the actual price is larger, equal or less than the threshold values.

TABLE I
PRICE DEFINITION

	$e_{i,t} \leq e_a$	$e_{i,t} > e_a$
Regular-time	p_1	p_1
Peak-time	p_2	$p_3 = f(e_{i,t})$

p_1 and p_2 are static, while p_3 is dynamic; and $p_1 < p_2 < p_3$.

TABLE II
FREQUENTLY USED NOTATIONS

$\mathcal{U}$	A utility company
$\mathcal{C}$	Community gateway (CG)
$U_1, \cdots, U_n$	n customers
$U'_1, \cdots, U'_n$	n customers ranked with $(1, \cdots, n)$ by $\mathcal{U}$
t	A time slot in time period T
$e_{i,t}$	The electricity usage of U_i during t
$e_{s,t}$	$= \sum_{i=1}^{n} e_{i,t}$, the community-wide electricity usage
e_m	The threshold value to determine peak time
e_a	The threshold value to set electricity price for customers
$f()$	The dynamic price function
p_1, p_2	Two static prices
p_3	Dynamic price
$E_{pk_i}()$	A homomorphic encryption function
$\tilde{p}_i$	The price threshold set by U_i
$e_{[1,\cdots,n]/i,t}$	A sum of electricity usage of customers except U_i

Electricity usage and electricity price are both tightly related to customer privacy, given that price is determined in accordance with usage. The utility company is a trusted entity and has full knowledge about the electricity usage of all the customers. It sets the electricity price for all the customers based on the data. The CG indicates the price information to individual customers. As a local device, the CG is not necessarily trustworthy, and should not know any customer's electricity usage and actual price. Thus, the issue of *privacy preservation* is to protect these two types of information from being disclosed to the CG and the compromised customers. It must be guaranteed before the strategy is pervasively adopted.

V. USAGE-BASED DYNAMIC PRICING

According to the DP strategy introduced in the previous section, we propose the UDP scheme with privacy preservation for smart grid. The operation of the scheme is composed of four phases as shown in Fig. 2. The utility company $\mathcal{U}$ first initializes the pricing parameters and passes them to the community gateway $\mathcal{C}$ and the customers. Specifically, it defines the usage threshold e_m according to the capacity of the local power grid in the community, and defines the dynamic price function $f()$ for peak time. Apparently, e_m may be different for different communities. For each community, $\mathcal{U}$ selects random secrets for $(U_1, \cdots, U_n)$ and $\mathcal{C}$.

After the system initialization, the customers report their electricity usage per time slot to $\mathcal{C}$. They mix their electricity usage with their secrets for privacy preservation. $\mathcal{C}$ removes the random secrets and obtains the community-wide electricity usage at each time slot. It returns a price indicator to the customer with respect to the community-wide electricity usage. Meanwhile, it forwards the received electricity usage,

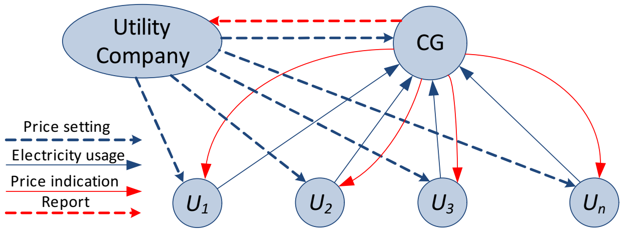


Fig. 2. Work flow of the UDP scheme

without modification, to $\mathcal{U}$ for billing and accounting. Because $\mathcal{U}$ knows the random secret of each customer, it is able to recover the individual electricity usage and compute the actual electricity price for each customer. Below, we elaborate on these phases.

A. System Initialization

The utility company $\mathcal{U}$, the community gateway $\mathcal{C}$ and all the customers $(U_1, \cdots, U_n)$ communicate to configure the system parameters for a specific time period $\mathcal{T}$.

a) Parameter setup.: $\mathcal{U}$ generates system parameters. It runs an HE generator $\mathcal{G}$ and obtains the HE parameters $(p, q, R, R_q, R_p, \chi)$. It then generates a cyclic group $\mathbb{G}'$ with order $\bar{p}$ where $\bar{p}$ is a large prime and the largest number in $\mathbb{G}'$ is $l \ll p$. It also generates two cyclic groups $\mathbb{G}$ and $\mathbb{G}_T$ with the same order $\bar{q}$, where $\bar{q}$ is a large prime. Suppose $\mathbb{G}$ and $\mathbb{G}_T$ are equipped with a pairing, i.e., a non-degenerated and efficiently computable bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ such that $i) \forall g, h \in \mathbb{G}, \forall a, b \in \mathbb{Z}_{\bar{q}}, e(g^a, h^b) = e(g, h)^{ab}$; and ii) $\exists g \in \mathbb{G}, e(g, g)$ has an order n in $\mathbb{G}_T$.

$\mathcal{U}$ generates $n+1$ distinct random numbers $g_j \in \mathbb{G}'$ for $0 \leq j \leq n$ $(g_{n+1} = g_0)$ and defines a cryptographic hash function $H : \{0,1\}^* \to \mathbb{Z}_{\bar{p}}$ and a keyed-hash message authentication code $HMAC$. Lastly, it publishes the system parameters $\mathcal{P} = (p, q, R, R_q, R_p, \chi, \bar{p}, \mathbb{G}', \bar{q}, e, \mathbb{G}, \mathbb{G}_T, H, HMAC)$.

b) Secret distribution.: $\mathcal{U}$ assigns secrets to $(U_1, \cdots, U_n)$ and $\mathcal{C}$. Specifically, it arranges customers $(U_1, \cdots, U_n)$ with ranks $(1, \cdots, n)$ at random. The customer with id_i at rank k obtains the secrets $(g_k, g_{k+1}, s_i = H(id_i)^s)$, where s is the master key of $\mathcal{U}$. The customers are not informed about their ranks. $\mathcal{U}$ further sends the secrets $(g_1, g_0, s_c = H(id_c)^s)$ to $\mathcal{C}$.

c) Price function.: $\mathcal{U}$ defines a price function and passes it to $\mathcal{C}$, who will use the function to determine dynamic price information for a given customer. In the proposed price function, price is determined by several factors, i.e., individual electricity usage $e_{i,t}$, the community-wide electricity usage $e_{s,t}$, threshold values (e_m, e_a), static prices (p_1, p_2), and the coefficients (a, b, c). $\mathcal{U}$ delivers $(e_m, e_a, p_1, p_2, a, b, c)$ to $\mathcal{C}$. In accordance with Table I, we define the price function $F(e_{i,t})$ as

$$F(e_{i,t}) = \begin{cases} p_1, & \text{if } e_{s,t} \leq e_m \\ p_2, & \text{if } e_{s,t} > e_m, e_{i,t} \leq e_a \\ a + be_{i,t} + ce_{i,t}^2, & \text{if } e_{s,t} > e_m, e_{i,t} > e_a \end{cases} \quad (1)$$

When $e_{i,t} \leq e_a$, U_i has static price p_1 or p_2. When $e_{i,t} > e_a$, the dynamic price is applied.

B. Electricity Usage Collection

We elaborate the electricity usage collection with respect to a time slot $t \in \mathcal{T}$ and a specific customer U_i at rank k. U_i reports its electricity usage $e_{i,t}$ and a price threshold $\tilde{p}_i$ to $\mathcal{C}$. To preserve its privacy, U_i executes the following steps:

1) calculate $\hat{e}_{i,t} = e_{i,t} + g_k^{H(t)} - g_{k+1}^{H(t)}$.
2) use the published system parameter $\mathcal{P}$ to generate an HE public/secret key pair (pk_i, sk_i).
3) use the homomorphic encryption to generate a 3-tuple $(pk_i, E_{pk_i}(e_i), E_{pk_i}(\tilde{p}_i))$.
4) generate $d_i = (\hat{e}_{i,t}, pk_i, E_{pk_i}(e_{i,t}), E_{pk_i}(\tilde{p}_i))$.
5) use the session key $\kappa = e(s_i, H(id_c)) = e(H(id_i), H(id_c))^s$, and generate the keyed-hash message authentication code $HMAC_\kappa(d_i)$.
6) send $r_i = (id_i, d_i, HMAC_\kappa(d_i))$ to $\mathcal{C}$.

C. Price Indication

The community gateway $\mathcal{C}$ receives all electricity usage reports r_i for $1 \leq i \leq n$. It does the following verification and calculation, and then sends a price indicator to the customer:

1) recover the session key $\kappa = e(H(id_i), s_c) = e(H(id_i), H(id_c))^s$, and verify the authenticity of d_i by $HMAC_\kappa(d_i)$.
2) retrieve $\hat{e}_{i,t}$ from d_i and calculate

$$\begin{aligned} \sum_{j=1}^{n} \hat{e}_{i,t} &= \sum_{j=1}^{n} (e_{i,t} + g_k^{H(t)} - g_{k+1}^{H(t)}) \\ &= \sum_{j=1}^{n} e_{i,t} + (g_1^{H(t)} - g_2^{H(t)} + \cdots - g_0^{H(t)}) \\ &= \sum_{j=1}^{n} e_{i,t} + (g_1^{H(t)} - g_0^{H(t)}) \end{aligned} \quad (2)$$

3) obtain $e_{s,t} = \sum_{j=1}^{n} \hat{e}_{i,t} - g_1^{H(t)} + g_0^{H(t)}$.
4) compare $e_{s,t}$ and e_m. If $e_{s,t} < e_m$, set $p_i = p_1$, send p_x to U_i, and stop; otherwise, compute p_i by the function $f()$ and continue with the following steps.
5) through the homomorphic encryption technique, obtain the $E_{pk_i}(\alpha)$ and $E_{pk_i}(\beta)$, where $\alpha = \tilde{p}_i$ and $\beta = a + be_{i,t} + ce_{i,t}^2$.
6) choose a random value $\varphi \in \mathbb{Z}_p$ such that $1 \leq \varphi < \lfloor p/(2l) \rfloor$ and $m | \varphi$, $m \in \mathbb{Z}$, $1 \leq m \leq l$, and calculate $ind_i = E_{pk_i}(\varphi(\alpha - \beta))$ from $E_{pk_i}(\alpha)$ and $E_{pk_i}(\beta)$.
7) finally return the price indicator ind_i to U_i.

For customer U_i, if it receives p_1, it will know the current price is the regular-time price. If it otherwise receives a price indicator ind_i, it will understand that the current price is a peak-time price and further decrypt ind_i to obtain the indicator $res_i = \varphi(\alpha - \beta)$. If $0 < res_i \leq \frac{p-1}{2}$, U_i concludes $\alpha \geq \beta$ and therefore $\tilde{p}_i > p_i$; if $res_i = 0$, U_i concludes $\tilde{p}_i = p_i$; if $\frac{p-1}{2} < res_i < p$, U_i obtains $\tilde{p}_i < p_i$.

Note that, $\varphi(\alpha - \beta)$ locates in the range $[-p/2, p/2)$. In this case, the comparison result of α and β implies that of $\tilde{p}_i$ and p_i. More analysis can be found in Sec. VII-A.

D. Report and Charge

The utility company $\mathcal{U}$ knows the secret keys of all the customers. With d_i sent from $\mathcal{C}$, $\mathcal{U}$ verifies the authenticity of d_i and obtains the actual electricity usage $e_{i,t}$ by removing the secret keys g_j for $0 \leq j \leq n$. Based on the actual electricity usage and the price function, $\mathcal{U}$ computes the electricity prices for the individual customers and charges them accordingly.

VI. Adaptation to Community Dynamics

The community network contains n customers initially. Over time, the number of customers may be changed because the residents may move in or out of the community. The proposed UDP scheme can easily adapt to the community dynamics through the following registration and deregistration.

A. Registration

When a new customer U_{n+1} registers to $\mathcal{U}$, $\mathcal{U}$ randomly picks a rank value $k^+ \in \{2, \cdots, n\}$ for U_{n+1}. Then, it adjusts the ranks of all existing customers in the community as follows: for any existing a customer in the community, its rank k^* remains unchanged if $1 \leq k^* < k^+$, or increased by 1 otherwise. After the adjustment, $\mathcal{U}$ generates secrets for U_{n+1} and updates the secrets of the two customers with new ranks $k^+ - 1$ and $k^+ + 1$. Other customers and $\mathcal{C}$ do not need to update secrets.

Specifically, $\mathcal{U}$ generates two secrets g'_{k^+} and g'_{k^++1} for U_{n+1}, replaces g_{k^+} with g'_{k^+} for the customer with new rank $k^+ - 1$, and replaces g_{k^+} with g'_{k^++1} for the customer with new rank $k^+ + 1$. Note that, if $\mathcal{U}$ assigns the new customer U_{n+1} with rank 1 or $n + 1$, $\mathcal{C}$ needs to change its secrets and such modification reveals U_{n+1}'s rank to $\mathcal{C}$. Therefore, we require $\mathcal{U}$ not to assign the new customer with rank 1 or $n + 1$.

However, if $\mathcal{C}$ compromises some customers, the secret change of these compromised customers would also reveal U_{n+1}'s rank information. One solution to resolve the rank disclosure problem is to enable simultaneous addition of multiple new customers. As such, multiple random ranks will be generated and assigned out, and the simultaneous change of secrets will make it difficult for $\mathcal{C}$ and the compromised customers to identify the rank of a specific customer.

B. Deregistration

If a customer U_i at rank k^- $(1 \leq k^- \leq n)$ de-registers to $\mathcal{U}$, $\mathcal{U}$ adjusts the ranks of other customers in the following way. For a customer with rank k^*, if $1 \leq k^* < k^-$, its rank remains unchanged; otherwise, it is decreased by 1. Afterwards, the secrets of these customers need the corresponding adjustment.

Specifically, if $k^- = 1$, $\mathcal{U}$ replaces g_1 with g_2 for $\mathcal{C}$; if $k^- = n$, it replaces g_0 with g_n for $\mathcal{C}$. In case of $2 \leq k^- \leq n - 1$, $\mathcal{U}$ replaces g_{k^-} with g_{k^-+1} for the customer at new rank $k^- - 1$. After making these changes, $\mathcal{C}$ can still obtain the community-wide electricity usage $e'_{s,t}$ of $n-1$ customers.

Note that, $\mathcal{C}$ and the customers with old ranks $k^- - 1$ and $k^- + 1$ may find their rank relations with the deregistered customer when their secrets are updated. The disclosed rank information cannot be used to violate the privacy of other registered customers. Besides, simultaneous deregistration can further prevent the customers who have their secrets changed from identifying the relations between their ranks and those of the deregistered customers.

VII. Privacy Analysis

In this section, we validate the privacy preservation property of the proposed UDP scheme. We assume that $\mathcal{U}$ is the only trusted entity, and we define two types of attackers with different targets.

A. Targeting on Community-wide Electricity Usage

We use the following theorem to prove the hardness of obtaining the community-wide electricity usage by the malicious customers.

Theorem 1: $\mathcal{C}$ does not disclose the community-wide electricity usage to an individual customer U_i.

Proof: In step 2 of price indication, $\mathcal{C}$ obtains the community-wide electricity usage $e_{s,t}$. Then, in the following steps, it generates two ciphertexts respectively for the plaintexts α and β. If $\mathcal{C}$ directly sends $E_{pk_i}(\alpha)$ and $E_{pk_i}(\beta)$ to U_i, U_i can derive the coefficients (a, b, c) and threshold values e_m, e_a, which is not necessary and insecure. In step 6, $\mathcal{C}$ sends $\varphi(\alpha - \beta)$ to U_i, where φ is a random number added for anonymity. Since $m|\varphi$ for some $1 \leq m \leq l$, we have $m|(\varphi(\alpha - \beta))$. $(\alpha - \beta)$ can be multiple possible values in U_i's view. Thus, the customers are unable to obtain price parameters and community-wide usage information $e_{s,t}$. ■

B. Targeting on Customer Electricity Usage

We discuss the privacy violation attacks which target on obtaining a given customer U_i's electricity usage $e_{i,t}$. We classify the attacks into four categories according the attackers' capabilities: i) single-customer launched; ii) multi-customer launched; iii) CG launched; and iv) customer-and-CG launched.

1) Single-customer Launched Attack: This attack is performed by a single compromised customer $U_j, j \neq i$ in the community. In the UDP scheme, U_j can obtain the customized price indicator, and knows when $e_{s,t} > e_m$ and $e_{i,t} > e_a$. However, $\mathcal{C}$ will not send back the community-wide usage $e_{s,t}$. In addition, $e_{s,t}$ contains the usage of multiple users. The electricity usage $e_{k,t}$ of any customer U_k for $k \neq i, j$ acts as random numbers to anoymize $e_{i,t}$. U_j cannot obtain any related information of $e_{i,t}$.

2) Multi-customer Launched Attack: In this attack, multiple compromised customers U_j for $j \in \mathcal{A}$ attempt to obtain $e_{i,t}$ through collusion. Likewise, they cannot obtain $e_{s,t}$. However, as the number of colluded customers increases, the randomness is reduced and the probability of having a correct guess on $e_{i,t}$ increases. In an extreme case that $n - 1$ customers are colluded, they are able to know the sum of their electricity usage $e_{[1,\cdots,n]/i,t}$ $(= e_{s,t} - e_{i,t})$. Since $e_{s,t} \leq e_m$ or $e_{s,t} > e_m$ is publicly known, they can derive whether $e_{i,t} \leq e_m - e_{[1,\cdots,n]/i,t}$ or $e_{i,t} > e_m - e_{[1,\cdots,n]/i,t}$. They can effectively narrow down the range of $e_{i,t}$ but cannot obtain exact value of $e_{i,t}$.

3) CG-launched Attack: This attack is launched by $\mathcal{C}$ alone, without involving any compromised customer. In the UDP scheme, U_i sends an electricity usage report to $\mathcal{C}$. However, the UDP scheme provides privacy preservation such that $\mathcal{C}$ is unable to obtain $e_{i,t}$. Recall that U_i transmits $\hat{e}_{i,t}$ and $E_{pk_i}(e_{i,t})$, where $\hat{e}_{i,t} = e_{i,t} + g_k^{H(t)} - g_{k+1}^{H(t)}$ and $E_{pk_i}()$ is a homomorphic encryption under public key pk_i. $E_{pk_i}(e_{i,t})$ reveals no information about $e_{i,t}$ to $\mathcal{C}$ because $\mathcal{C}$ does not have the HE secret key sk_i. As for $\hat{e}_{i,t}$, since $\mathcal{C}$ only obtains the secrets g_1 and g_0 from $\mathcal{U}$, it cannot get both g_k and g_{k+1}. If $g_k(g_{k+1})$ is known to $\mathcal{C}$, $g_{k+1}^{H(t)}(g_k^{H(t)})$ appears as a random number to anonymize $e_{i,t}$. Thus, $e_{i,t}$ cannot be obtained by $\mathcal{C}$.

4) customer-and-CG-launched Attack: This attack is a combination of the previous two attacks. It involves $\mathcal{C}$ and one or multiple compromised customers. Denote the number of colluded customers by $1 \le \theta \le n-2$. We do not consider the case $\theta = n-1$, where $\mathcal{C}$ can easily obtain $e_{i,t} = e_{s,t} - e_{[1,\cdots,n]/i,t}$. Similar to the existed privacy analysis [27], the privacy of $e_{i,t}$ can be regarded as uncertainty from attackers' point of view. The more uncertainty imposed to the attackers, the more privacy preserved. Below, we analyze the uncertainty of $e_{i,t}$ from attackers' perspective, i.e. the probability of having a correct guess on $e_{i,t}$. It remains important to know that nobody but $\mathcal{U}$ knows the rank of any customer in the community.

If $\mathcal{C}$ compromises two rank-adjacent customers, e.g. two customers respectively with ranks k^* and k^*+1, it will be able to find that g_{k+1} is the common secret of the two customers and realize that the rank of one customer equals to the rank of the other minus 1. If $\mathcal{C}$ compromises three rank-adjacent customers, e.g. three customers with rank k^*-1, k^*, and k^*+1, it can correctly sort the ranks of these three customers. Then, it will not use the secrets of the customer at rank k^* in the guessing process because the customer does not share any common secret with the target customer U_i.

Suppose that U_i has a rank k. We regard $\mathcal{C}$ as a compromised customer U'_0. U'_x denotes the customer with rank x. Then, other customers and $\mathcal{C}$ can be sorted in a chain according to their secret structure as follows:

$$U'_{k+1}, U'_{k+2}, \cdots, U'_n, U'_0(\mathcal{C}), U'_1, \cdots, U'_{k-1}.$$

Without knowing the rank information, $\mathcal{C}$ is unaware of its own position and any compromised customer's position in this chain. We take a sequence of consecutive compromised customers as a fragment. The chain may contain multiple compromised fragments, and there is no overlapping between any two fragments. We first solve the following problem: if $\mathcal{C}$ compromises $1 < \theta < n$ customers from the chain, how many fragments will it form? This problem is critical because only the end customers of a fragment are able to contribute to the attack effectively.

Denote by δ the number of fragments. We make the following notations to represent the number of possibilities:

- $\phi(n,\theta)$: θ out of n customers are compromised, i.e. $\binom{n}{\theta}$.
  - $\phi_r(n,\theta,\delta)$: δ fragments are formed.
    - $\phi_1(n,\theta,\delta)$: both U'_{k+1} and U'_{k-1} are compromised.
    - $\phi_2(n,\theta,\delta)$: U'_{k+1} is compromised, while U'_{k-1} is not.
    - $\phi_3(n,\theta,\delta)$: U'_{k+1} is not compromised, while U'_{k-1} is.
    - $\phi_4(n,\theta,\delta)$: neither U'_{k+1} nor U'_{k-1} is compromised.

We have $\phi_2 = \phi_3$ and the following recursive equations:

$$\begin{aligned} \phi_r &= \phi_1 + 2\phi_2 + \phi_4; \\ \phi_4(n,\theta,\delta) &= \phi_r(n-2,\theta,\delta); \\ \phi_1(n,\theta,\delta) &= \phi_1(n-2,\theta-2,\delta) + \phi_4(n-2,\theta-2,\delta-2) \\ &\quad + 2\phi_2(n-2,\theta-2,\delta-1); \\ \phi_2(n,\theta,\delta) &= \phi_1(n-1,\theta,\delta) + \phi_2(n-1,\theta,\delta). \end{aligned} \tag{3}$$

These equations are associated with the following facts:

- if $\delta = 1$, then
$$\begin{aligned} \phi_r(n,\theta,\delta) &= n-\theta+1, \\ \phi_1(n,\theta,\delta) &= 0, \\ \phi_2(n,\theta,\delta) &= 1, \\ \phi_4(n,\theta,\delta) &= n-\theta-1; \end{aligned} \tag{4}$$
- if $\theta = \delta$, then
$$\begin{aligned} \phi_r(n,\theta,\delta) &= \tbinom{n-\theta+1}{\theta}, \\ \phi_1(n,\theta,\delta) &= \tbinom{n-\theta-1}{\theta-2}, \\ \phi_2(n,\theta,\delta) &= \tbinom{n-\theta-1}{\theta-1}, \\ \phi_4(n,\theta,\delta) &= \tbinom{n-\theta-1}{\theta}; \end{aligned} \tag{5}$$
- if $n = \theta + \delta - 1$, then
$$\begin{aligned} \phi_r(n,\theta,\delta) = \phi_1(n,\theta,\delta) &= \tbinom{\theta-1}{\delta-1}, \\ \phi_2(n,\theta,\delta) = \phi_4(n,\theta,\delta) &= 0; \end{aligned} \tag{6}$$
- if $n < \theta + \delta - 1$ or $\theta < \delta$, then
$$\phi_r(n,\theta,\delta) = \phi_1(n,\theta,\delta) = \phi_2(n,\theta,\delta) = \phi_4(n,\theta,\delta) = 0. \tag{7}$$

We consider only the case of $\delta > 1$ because for $\delta = 1$, $\mathcal{C}$ has to compromise all the $n-1$ customers including U'_{k+1} and U'_{k-1} in order to obtain $e_{i,t}$. In the guessing process, $\mathcal{C}$ will make $\delta(\delta-1)$ distinct calculations, each involving the header of one fragment and the tailer of another fragment. Thus, the probability of having a correct guess on $e_{i,t}$ is

$$p_{succ}(n,\theta) = \sum_{\delta=2}^{\theta} \frac{1}{\delta(\delta-1)} \cdot \frac{\phi_1(n,\theta,\delta)}{\binom{n}{\theta}} \tag{8}$$

In Fig. 3, we plot $p_{succ}(n,\theta)$ where $n = \{20, 25, \cdots, 90\}$ and $\theta = \{6, 7, \cdots, 20\}$. It can be seen that when $\mathcal{C}$ compromises 19 customers (totally 20 including itself), the probability of having a correct guess reaches the upper bound 100% ($ln(10^4) = 9.21$). The success probability significantly decreases as the number of the total customers increases or the number of the compromised customers decreases. For example, $p_{succ}(40,20) = 0.9\%$ and $p_{succ}(90,10) = 0.016\%$. We consider the electricity usage normally varies in a fixed range, and the number of possible values of the electricity usage is less than 100, the probability of having a correct guess for the

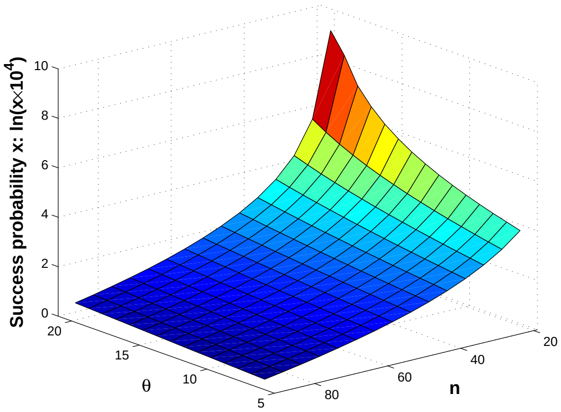


Fig. 3. Success probability $p_{succ}(n,\theta)$

above two cases can be negligible due to $0.016\% < 0.9\% < 1\%$. Therefore, such attack can be effectively prevented by adopting the privacy-preserving techiniques embedded into the UDP scheme.

VIII. Privacy Enhancement

In previous sections, we have presented the UDP scheme where a customer U_i has 2 secrets (thus secret-size 2) and the secrets are shared with the two customers at adjacent ranks. We call such secret structure as 1-step secret structure, shown in Fig. 4(a). In Fig. 4, the black dot represents the CG and other circles represent the customers. In this section, we enhance the privacy preservation capability of the UDP scheme by replacing the 1-step secret structure with w structures for $w \geq 2$, and increasing the secret size from 2 to $2w$.

Figures 4(b) and 4(c) show the 2-step and 3-step structures, respectively. When multiple secret structures are applied, the secrets are independently generated for each structure. In the 2-step structure, $\mathcal{U}$ assigns U_i with secrets g_i and g_{i+2} (different from those assigned in the 1-step structure). This makes the secrets of U_{i-2}, U_i, U_{i+2} dependent on each other. Here, the index is calculated based on modular $n+1$. Since the number of the total customers is n, the w-step structure is identical to the $(n+1-w)$-step structure. The number of step structures for achieving the highest privacy level is $w = \lceil \frac{n}{2} \rceil$. The smaller w, the less privacy preservation. In the following, we focus on the extended UDP (eUDP) scheme which uses $\lceil \frac{n}{2} \rceil$ secret structures to achieve highest privacy level.

To enable the $\lceil \frac{n}{2} \rceil$-step secret structure, $\mathcal{U}$ generates secrets $g_{w,0}, g_{w,1}, \cdots, g_{w,n}$ for $w = 1, \cdots, \lceil \frac{n}{2} \rceil$. It assigns the rank-$k$ customer U_i with $(g_{1,k}, g_{1,k+1}), \cdots, (g_{w,k}, g_{w,k+w})$. The index is calculated through modular $n+1$ operation. Thus, U_i obtains $2 * \lceil \frac{n}{2} \rceil$ elements as its secrets. It generates $\hat{e}_{i,t}$ as

$$\hat{e}_{i,t} = e_{i,t} + \sum_{j=1}^{w} (g_{j,k}^{H(t)} - g_{j,k+j}^{H(t)}) \tag{9}$$

Clearly, $\mathcal{C}$ is able to calculate

$$e_{s,t} = \sum_{i=1}^{n} e_{i,t} = \sum_{i=1}^{n} \hat{e}_{i,t} - \sum_{i=1}^{w} (g_{i,0}^{H(t)} - g_{i,i}^{H(t)}). \tag{10}$$

where $g_{i,0}$ and $g_{i,i}$ for $1 \leq i \leq w$ are the secrets of $\mathcal{C}$.

a) Sub-circle problem: When the largest common factor of w and $n+1$ is not equal to 1, sub-circles are formed in the w-step secret structure. In this case, $\mathcal{C}$ has additional knowledge about the secret structures among customers; it knows that the secrets from the customers who are not in a sub-circle with the target customer are not useful in the guessing process. Thus, $\mathcal{C}$ can increase the probability of having a correct guess. We provide a simple solution to resolve this problem as follows: $\mathcal{U}$ creates Δn dummy customers such that the largest common factor of m and $n + \Delta n$ is equal to 1, and it randomly ranks these dummy customers; then, in the w-step secret structure, it generates secrets for $(n + \Delta n)$ customers, and sends all the secrets of the dummy customers to $\mathcal{C}$. The secret size of each customer remains the same, but $\mathcal{C}$ needs extra storage for the secrets of the dummy customers. By using the dummy customers, the w-step secret structure does not contain any sub-circle.

b) Privacy analysis: The following theorem implies that the enhanced scheme with $\lceil \frac{n}{2} \rceil$ secret structures achieves the highest privacy level, i.e. $\mathcal{C}$ has the lowest probability of having a correct guess on $e_{i,t}$.

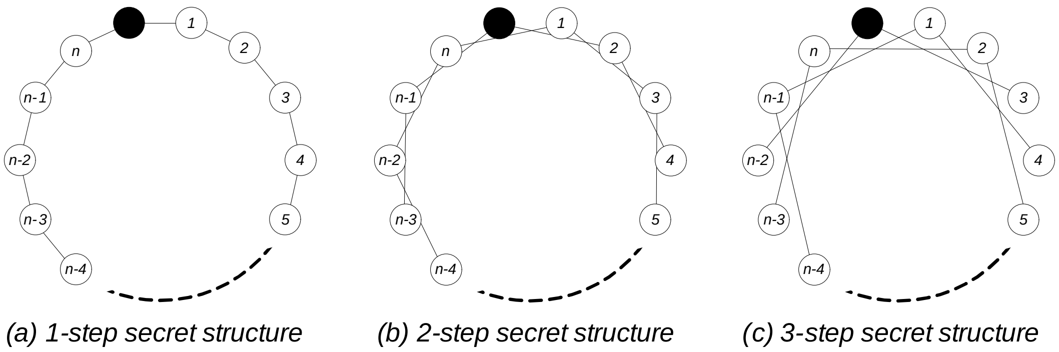
Theorem 2: In the eUDP scheme, if $\mathcal{C}$ compromises less than $n-1$ customers, it always has lowest probability of having a correct guess on $e_{i,t}$.

Proof: Since $\mathcal{C}$ compromises less than $n-1$ customers, there exists a non-compromised customer U_j $(j \neq i)$. Denote the ranks of U_i and U_j respectively by k and k'. We consider $k > k'$ first. If $0 < k - k' \leq \lceil \frac{n}{2} \rceil$, in the $(k-k')$-step structure, U_j has secrets $g_{k'}$ and $g_{k'+k-k'} = g_k$ while U_i has secret g_k, and the value $g_k^{H(t)}$ is embedded in $\hat{e}_{i,t}$ and can be removed collectively only by U_i and U_j. Without U_j's help, $\mathcal{C}$ cannot obtain $e_{i,t}$. If $\lceil \frac{n}{2} \rceil < k - k' \leq n+1$, we have $2 \leq n+1-k+k' < n+1-\lceil \frac{n}{2} \rceil \leq n - \lceil \frac{n}{2} \rceil \leq \lceil \frac{n}{2} \rceil$. Thus, in the $(n+1-k+k')$-step secret structure, U_i has secrets g_k and $g_{k+n+1-k+k'} = g_{k'}$ while U_j has secret $g_{k'}$. Likewise, without compromising U_j, $g_{k'}^{H(t)}$ is a random number that cannot be deleted from $\hat{e}_{i,t}$, and thus $\mathcal{C}$ is unable to obtain $e_{i,t}$. In case of $k < k'$, the $(k'-k)$-step secret structure can protect $e_{i,t}$ from being obtained by $\mathcal{C}$ and the compromised customers. ■

c) Efficiency analysis: The eUDP scheme employs more secret structures than the UDP scheme to achieve higher privacy level. It requires more computation costs of all the entities and more communication overhead between $\mathcal{U}$ and the customers. It also requires the customers to be equipped with larger storage device for the secrets. Specifically, since only extra addition operations are required, the increased computation costs at the CG are negligible. For the communication overhead in the eUDP scheme, $\mathcal{U}$ needs to send $2 * \lceil \frac{n}{2} \rceil$ secrets, the size of which is $\lceil \frac{n}{2} \rceil$ times of that in the UDP scheme. The registration and deregistration in the eUDP scheme require more computation and communication effort which is $\lceil \frac{n}{2} \rceil$ times of that in the UDP scheme.

IX. Conclusion

In this paper, we have proposed a usage-based dynamic pricing (UDP) scheme for smart grid in a community environment. The UDP scheme enables the community gateway to



(a) 1-step secret structure (b) 2-step secret structure (c) 3-step secret structure

Fig. 4. Secret structures

send the price indication to the individual customers according to their individual electricity usage and the community-wide electricity usage in real time. It also preserves the privacy of the customers, i.e., to restrict the disclosure of the individual electricity usage to the community gateway. An extended version, named eUDP, with multiple secret structures is further presented to achieve the higher privacy level at the cost of additional computation and communication overhead. In the proposed dynamic pricing schemes, the dynamic price function $f()$ can be composed of addition and multiplication operations due to the limitation of homomorphic encryption techniques. For our future work, we will study the price function in practice and explore an extended construction of the price function while preserving the privacy of the customers.

REFERENCES

[1] Z. M. Fadlullah, M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, "Toward intelligent machine-to-machine communications in smart grid," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 60–65, 2011.

[2] M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 675–685, 2011.

[3] H. Liang, B. J. Choi, A. Abdrabou, W. Zhuang, and X. S. Shen, "Decentralized economic dispatch in microgrids via heterogeneous wireless networks," *IEEE JSAC*, vol. 30, no. 6, pp. 1061–1074, 2012.

[4] T. T. Kim and H. V. Poor, "Scheduling power consumption with price uncertainty," *IEEE Transactions on Smart Grid*, vol. 2, no. 3, pp. 519–527, 2011.

[5] I. Paschalidis, B. Li, and M. Caramanis, "Demand-side management for regulation service provisioning through internal pricing," *IEEE Transactions on Power Systems*, vol. 27, no. 3, pp. 1531–1539, 2011.

[6] J. Li, Z. Li, K. Ren, and X. Liu, "Towards optimal electric demand management for internet data centers," *IEEE Transactions on Smart Grid*, vol. 3, no. 1, pp. 183–192, 2012.

[7] "Electric utility," *Wikipedia*, http://en.wikipedia.org/wiki/Electric_utility.

[8] G. Kalogridis, R. Cepeda, S. Z. Denic, T. A. Lewis, and C. Efthymiou, "Elecprivacy: Evaluating the privacy protection of electricity management algorithms," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 750–758, 2011.

[9] A. H. M. Rad, V. W. S. Wong, J. Jatskevich, R. Schober, and A. Leon-Garcia, "Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid," *IEEE Transactions on Smart Grid*, vol. 1, no. 3, pp. 320–331, 2010.

[10] A. Lee and T. Brewer, "Smart grid cyber security strategy and requirements," *NISTIR 7628, 2nd Draft*.

[11] A. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 667–674, 2011.

[12] H. Cheung, A. Hamlyn, T. Mander, C. Yang, and R. Cheung, "Role-based model security access control for smart power-grids computer networks," in *Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century*, 2008, pp. 1–7.

[13] N. Ruiz, I. Cobelo, and J. Oyarzabal, "A direct load control model for virtual power plant management," *IEEE Transactions on Power Systems*, vol. 24, no. 2, pp. 959–966, 2009.

[14] "Hydro one," *http://www.hydroone.com/Pages/Default.aspx*.

[15] "Waterloo north hydro," *http://www.wnhydro.com/*.

[16] "The Smart Grid: An Introduction," U.S. Department of Energy, 2008.

[17] H. Khurana, M. Hadley, N. Lu, and D. Frincke, "Smart-grid security issues," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 81–85, 2010.

[18] X. Li, X. Liang, R. Lu, X. Lin, H. Zhu, and X. Shen, "Securing smart grid: Cyber attacks, countermeasures and challenges," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 38–45, 2012.

[19] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, 2012.

[20] G. Acs and C. Castelluccia, "I have a dream! (differentially private smart metering)," *Information Hiding*, vol. 6958, pp. 118 – 132, 2011.

[21] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?" in *Proceedings of the 3rd ACM Cloud Computing Security Workshop*, 2011, pp. 113–124.

[22] Y.-J. Kim, M. Thottan, V. Kolesnikov, and W. Lee, "A secure decentralized data-centric information infrastructure for smart grid," *IEEE Communications Magazine*, vol. 48, no. 11, pp. 58–65, 2010.

[23] Z. M. Fadlullah, M. Fouda, N. Kato, X. Shen, and Y. Nozaki, "An early warning system against malicious activities for smart grid communications," *IEEE Network*, vol. 25, no. 5, pp. 50–55, 2011.

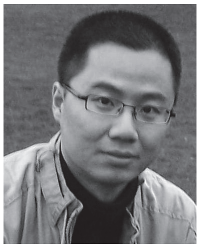
[24] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, "Smart community: an internet of things application," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 68–75, 2011.

[25] J. Park, Y. Kim, I. Eom, and K. Lee, "Economic load dispatch for piecewise quadratic cost function using hopfield neural network," *IEEE Transactions on Power Systems*, vol. 8, no. 3, pp. 1030–1038, 1993.

[26] H. Yamin, S. Al-Agtash, and M. Shahidehpour, "Security-constrained optimal generation scheduling for gencos," *IEEE Transactions on Power Systems*, vol. 19, no. 3, pp. 1365–1372, 2004.

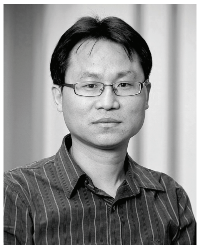
[27] L. Sweeney *et al.*, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty Fuzziness and Knowledge Based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

Xiaohui Liang (IEEE S'10) received the B.Sc. degree in Computer Science and Engineering and the M.Sc. degree in Computer Software and Theory from Shanghai Jiao Tong University (SJTU), China, in 2006 and 2009, respectively. He is currently working toward a Ph.D. degree in the Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research interests include applied cryptography, and security and privacy issues for e-healthcare system, cloud computing, mobile social networks, and smart grid.



Xu Li is a research engineer at Huawei Technologies Canada. Prior to joining Huawei, he worked at Inria, France (2011-2012) as research scientist, and at the University of Waterloo (2010-2011) and the University of Ottawa (2009-2010) as post-doc fellow. He received a PhD (2008) degree from Carleton University, an M.Sc. (2005) degree from the University of Ottawa, and a B.Sc. (1998) degree from Jilin University, China, all in computer science. During 2004.1-8, he held a visiting researcher position at National Research Council Canada. His research interests are in next-generation wireless networks, with over 70 refereed publications. He is on the editorial boards of the IEEE Transactions on Parallel and Distributed Systems, the Wiley Transactions on Emerging Telecommunications Technologies, Ad Hoc & Sensor Wireless Networks, and Parallel and Distributed computing and Networks. He is/was a guest editor of a number of international archive journals. He was a recipient of NSERC PDF awards and a number of other awards.

Rongxing Lu (IEEE S'09-M'11) received the Ph.D. degree in computer science from Shanghai Jiao Tong University, Shanghai, China in 2006 and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2012. He is currently a Postdoctoral Fellow with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and trusted computing.



Xiaodong Lin (IEEE S'07-M'09) received the Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1998 and the Ph.D. degree (with Outstanding Achievement in Graduate Studies Award) in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2008. He is currently an assistant professor of information security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON, Canada. His research interests include wireless network security, applied cryptography, computer forensics, software security, and wireless networking and mobile computing. Dr. Lin was the recipient of a Natural Sciences and Engineering Research Council of Canada (NSERC) Canada Graduate Scholarships (CGS) Doctoral and the Best Paper Awards of the 18th International Conference on Computer Communications and Networks (ICCCN 2009), the 5th International Conference on Body Area Networks (BodyNets 2010), and IEEE International Conference on Communications (ICC 2007).

Xuemin (Sherman) Shen (IEEE M'97-SM'02-F09) received the B.Sc.(1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a Professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo, Canada. He was the Associate Chair for Graduate Studies from 2004 to 2008. Dr. Shen's research focuses on resource management in interconnected wireless/wired networks, wireless network security, wireless body area networks, vehicular ad hoc and sensor networks. He is a co-author/editor of six books, and has published more than 600 papers and book chapters in wireless communications and networks, control and filtering. Dr. Shen served as the Technical Program Committee Chair for IEEE VTC'10 Fall, the Symposia Chair for IEEE ICC'10, the Tutorial Chair for IEEE VTC'11 Spring and IEEE ICC'08, the Technical Program Committee Chair for IEEE Globecom'07, the General Co-Chair for Chinacom'07 and QShine'06, the Chair for IEEE Communications Society Technical Committee on Wireless Communications, and P2P Communications and Networking. He also serves/served as the Editor-in-Chief for IEEE Network, Peer-to-Peer Networking and Application, and IET Communications; a Founding Area Editor for IEEE Transactions on Wireless Communications; an Associate Editor for IEEE Transactions on Vehicular Technology, Computer Networks, and ACM/Wireless Networks, etc.; and the Guest Editor for IEEE JSAC, IEEE Wireless Communications, IEEE Communications Magazine, and ACM Mobile Networks and Applications, etc. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004, 2007 and 2010 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. Dr. Shen is a registered Professional Engineer of Ontario, Canada, an IEEE Fellow, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, and a Distinguished Lecturer of IEEE Vehicular Technology Society and Communications Society. Dr. Shen has been a guest professor of Tsinghua University, Shanghai Jiao Tong University, Zhejiang University, Beijing Jiao Tong University, Northeast University, etc.