Smart Meter Privacy Based on Adversarial Hypothesis Testing

Zuxing Li*, Tobias J. Oechtering*, and Deniz Gündüz†
*School of Electrical Engineering, KTH Royal Institute of Technology, Stockholm, Sweden
†Department of Electrical and Electronic Engineering, Imperial College London, London, United Kingdom

***Abstract*—Privacy-preserving energy management is studied in the presence of a renewable energy source. It is assumed that the energy demand/supply from the energy provider is tracked by a smart meter. The resulting privacy leakage is measured through the probabilities of error in a binary hypothesis test, which tries to detect the consumer behavior based on the meter readings. An optimal privacy-preserving energy management policy maximizes the minimal Type II probability of error subject to a constraint on the Type I probability of error. When the privacy-preserving energy management policy is based on all the available information of energy demands, energy supplies, and hypothesis, the asymptotic exponential decay rate of the maximum minimal Type II probability of error is characterized by a divergence rate expression. Two special privacy-preserving energy management policies, the memoryless hypothesis-aware policy and the hypothesis-unaware policy with memory, are then considered and their performances are compared. Further, it is shown that the energy supply alphabet can be constrained to the energy demand alphabet without loss of optimality for the evaluation of a single-letter-divergence privacy-preserving guarantee.**

I. Introduction

Real-time information about energy demands and advanced control and communication technologies enable more efficient energy generation and distribution in smart grids [1]. Real-time energy demand information is provided to the energy provider (EP) by the smart meters installed at consumer premises. While high-resolution meter readings are essential for monitoring and control tasks, they also reveal sensitive private information about the consumers [2], [3]. A number of privacy-preserving technologies have been developed for the smart meter privacy problem in the recent years. In [4], an encryption method is proposed to protect the privacy of an individual consumer through data aggregation in the neighborhood. In [5], a privacy scheme is devised by scheduling delay-tolerable appliances to hide the energy demand profiles of others. While most of the literature focuses on the manipulation of meter readings to preserve privacy, there is a growing interest in guaranteeing privacy by directly altering the energy demands from the EP. This can be achieved by exploiting renewable energy sources (RESs) or energy storage devices to filter the real energy demand characteristics. Information-theoretic approaches to these problems have been studied in [1], [6]–[9].

The work has been supported by the Swedish Research Council (VR) under Grant 2015-06815 and the UK Engineering and Physical Sciences Research Council (EPSRC) under Grant EP/N021738/1 within the CHIST-ERA project COPES.

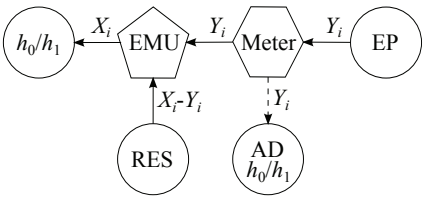

Fig. 1. The model of the smart meter privacy problem in the presence of a renewable energy source (RES), where energy and information flows are represented by solid and dashed arrows, respectively.

In this paper, we consider the smart meter privacy leakage to an informed adversary (AD), for instance the EP. In particular, we study the optimal privacy-preserving energy management policy in the presence of a RES following [1], [7], [9]. However, different from these works, we measure the smart meter privacy leakage by the probability of error in a Neyman-Pearson hypothesis test performed by the AD. Hypothesis testing models of privacy leakage have been studied in other contexts [10]–[15], e.g., in sensor networks and multimedia forensics. In this work, we characterize the asymptotic exponential decay rate of the maximum minimal Type II probability of error by a Kullback-Leibler divergence rate expression. We also consider two distinct privacy-preserving energy management policies: a memoryless hypothesis-aware policy and a hypothesis-unaware policy with memory. We further show that the optimal memoryless hypothesis-aware policy cannot outperform the optimal hypothesis-unaware policy with memory.

Due to the space limitation, some proofs are omitted in this paper. They will be presented in a journal [16] in preparation.

II. System Model and Privacy-Preserving Energy Management Policy

The considered smart meter privacy model is shown in Fig. 1. The private consumer behavior is modeled by the binary hypothesis H which can be h_0 or h_1. In the following, we use the short notation $\cdot|h_j$ for $\cdot|H = h_j$, $j \in \{0,1\}$, to denote a random variable conditioned on hypothesis h_j. Under hypothesis h_0 (resp. h_1), the energy demand X_i at time slot i is independently and identically distributed (i.i.d.) according to $p_{X|h_0}$ (resp. $p_{X|h_1}$) and defined on the finite alphabet $\mathcal{X}$. In this paper, $p_{X|h_0}$ and $p_{X|h_1}$ satisfy $\mathrm{D}(p_{X|h_0}||p_{X|h_1}) > 0$; $\min \mathcal{X} \geq 0$; and $\max \mathcal{X} < \infty$. At any time slot i, the energy management unit (EMU) follows a random energy

management policy γ_i to determine the energy supply y_i from the EP based on the demands x^i, the supplies y^{i-1}, and the correct hypothesis h as

$$\gamma_i : \mathcal{X}^i \times \mathcal{Y}^{i-1} \times \mathcal{H} \to \mathcal{Y} \big| \, x_i - y_i \geq 0, \tag{1}$$

where $\mathcal{Y}$ denotes the finite energy supply alphabet from the EP at any time slot with $\mathcal{Y} \supseteq \mathcal{X}$, $\min \mathcal{Y} = 0$, $\max \mathcal{Y} = \max \mathcal{X}$; the instantaneous constraint $x_i - y_i \geq 0$ imposes nonnegative energy supply from the RES at any time slot i. Let $\gamma^n \triangleq \{\gamma_i\}_{i=1}^n : \mathcal{X}^n \times \mathcal{H} \to \mathcal{Y}^n$ denote an energy management policy over an n-slot time horizon. We assume that the RES has an average energy generation rate of s and is equipped with a sufficiently large energy storage. Therefore, we only consider an average energy constraint as

$$\mathrm{E}\left[\frac{1}{n}\sum_{i=1}^{n}(X_i - Y_i)\middle| h_j\right] \leq s, \ j = 0, 1. \tag{2}$$

An energy management policy over an n-slot time horizon that satisfies (2) is denoted by $\gamma^n(s)$.

We consider that an AD, which can be the EP, has access to the meter readings y^n, and is fully informed about the energy demand statistics as well as the used energy management policy, i.e., the AD knows $p_{X^n|h_0}$, $p_{X^n|h_1}$, $\gamma^n(s)$, and therefore the corresponding $p_{Y^n|h_0}$, $p_{Y^n|h_1}$. The smart meter privacy leakage is modeled as a Neyman-Pearson test by the informed AD on the binary hypothesis. We define the minimal Type II probability of error of the AD under an upper bound constraint on the Type I probability of error as

$$\beta(n, \varepsilon, \gamma^n(s)) \triangleq \min_{\mathcal{A}_n \subseteq \mathcal{Y}^n} \{p_{Y^n|h_1}(\mathcal{A}_n) | p_{Y^n|h_0}(\mathcal{A}_n^c) \leq \varepsilon\},$$

where $\mathcal{A}_n$ denotes the decision region for h_0 of the AD. The privacy-preserving objective of the EMU is to maximize the probability of error of the AD. More specifically, for a given RES energy generation rate s, the EMU uses the optimal energy management policy to achieve the maximum minimal Type II probability of error subject to a Type I probability of error constraint

$$\beta_s(n, \varepsilon) \triangleq \max_{\gamma^n(s)} \{\beta(n, \varepsilon, \gamma^n(s))\}. \tag{3}$$

III. Asymptotic Characteristics of Privacy-Preserving Energy Management Policy

In the following, the optimal privacy-preserving energy management policy is characterized in the asymptotic regime as $n \to \infty$, by focusing on the asymptotic exponential decay rate of the maximum minimal Type II probability of error subject to a Type I probability of error constraint.

Define $\theta(s)$ as

$$\theta(s) \triangleq \inf_{k, \gamma^k(s)} \left\{\frac{1}{k}\mathrm{D}(p_{Y^k|h_0} || p_{Y^k|h_1})\right\}, \tag{4}$$

where the infimum is taken over all $k \in \mathbb{Z}_+$, and for each k, over all energy management policies that satisfy the average energy constraint over a k-slot time horizon.

Lemma 1.

$$\theta(s) = \lim_{k \to \infty} \inf_{\gamma^k(s)} \left\{\frac{1}{k}\mathrm{D}(p_{Y^k|h_0} || p_{Y^k|h_1})\right\}.$$

The proof of Lemma 1 is presented in [16]. It follows from the *subadditivity* of the sequence of $\inf_{\gamma^k(s)} \left\{\mathrm{D}(p_{Y^k|h_0} || p_{Y^k|h_1})\right\}$ and Fekete's lemma [17, Lemma 11.2].

Next, it is shown that the asymptotic exponential decay rate of the maximum minimal Type II probability of error subject to a Type I probability of error constraint can be characterized by $\theta(s)$.

Theorem 1. *Given $s > 0$,*

$$\limsup_{n \to \infty} \frac{1}{n} \log \frac{1}{\beta_s(n, \varepsilon)} \leq \theta(s), \ \forall \varepsilon \in (0, 1), \tag{5}$$

and

$$\lim_{\varepsilon \to 1} \liminf_{n \to \infty} \frac{1}{n} \log \frac{1}{\beta_s(n, \varepsilon)} \geq \theta(s). \tag{6}$$

Proof: Given any $k \in \mathbb{Z}_+$, $\gamma^k(s)$, and the resulting $p_{Y^k|h_0}$, $p_{Y^k|h_1}$, let $\gamma^{kl}(s)$ denote an energy management policy which repeatedly uses $\gamma^k(s)$ for l times. From the definition in (3) and Stein's lemma [18, Theorem 11.8.3], it follows

$$\begin{aligned}\limsup_{l \to \infty} \frac{1}{kl} \log \frac{1}{\beta_s(kl, \varepsilon)} &\leq \lim_{l \to \infty} \frac{1}{kl} \log \frac{1}{\beta(kl, \varepsilon, \gamma^{kl}(s))} \\ &= \frac{1}{k}\mathrm{D}(p_{Y^k|h_0} || p_{Y^k|h_1}),\end{aligned}$$

for all $\varepsilon \in (0, 1)$. Since for $k(l-1) < n \leq kl$ we have

$$\beta_s(kl, \varepsilon) \leq \beta_s(n, \varepsilon) \leq \beta_s(k(l-1), \varepsilon),$$

it follows

$$\limsup_{n \to \infty} \frac{1}{n} \log \frac{1}{\beta_s(n, \varepsilon)} \leq \frac{1}{k}\mathrm{D}(p_{Y^k|h_0} || p_{Y^k|h_1}),$$

for all $\varepsilon \in (0, 1)$, $k \in \mathbb{Z}_+$, and $\gamma^k(s)$. Therefore, we have

$$\limsup_{n \to \infty} \frac{1}{n} \log \frac{1}{\beta_s(n, \varepsilon)} \leq \theta(s), \ \forall \varepsilon \in (0, 1).$$

Given any $n \in \mathbb{Z}_+$, suppose that $\gamma^{n*}(s)$ leads to $p^*_{Y^n|h_0}$, $p^*_{Y^n|h_1}$, and achieves $\beta_s(n, \varepsilon')$, where the Type I probability of error upper bound ε' is equal to

$$\max_{\gamma^n(s)} \left\{p_{Y^n|h_0}\left\{y^n \middle| \log \frac{p_{Y^n|h_0}(y^n)}{p_{Y^n|h_1}(y^n)} < \mathrm{D}\left(p_{Y^n|h_0} || p_{Y^n|h_1}\right)\right\}\right\}.$$

If the AD uses the following hypothesis test strategy

$$\mathcal{A}_n = \left\{y^n \middle| \frac{1}{n} \log \frac{p^*_{Y^n|h_0}(y^n)}{p^*_{Y^n|h_1}(y^n)} \geq t\right\}, \tag{7}$$

where the test threshold t is

$$t = \frac{1}{n}\mathrm{D}(p^*_{Y^n|h_0} || p^*_{Y^n|h_1}), \tag{8}$$

from the definition of ε', the corresponding Type I probability of error satisfies the upper bound constraint

$$p^*_{Y^n|h_0}(\mathcal{A}_n^c) \leq \varepsilon'.$$

Since the hypothesis test strategy in (7) is not necessarily optimal for the AD, the definition of the maximum minimal Type II probability of error implies that

$$\beta_s(n, \varepsilon') \leq p^*_{Y^n|h_1}(\mathcal{A}_n). \tag{9}$$

Let $\varepsilon \to 1$ such that $\varepsilon \geq \varepsilon'$. We have

$$\lim_{\varepsilon \to 1} \beta_s(n, \varepsilon) \leq \beta_s(n, \varepsilon'). \tag{10}$$

In [19, Lemma 4.1.1], it has been shown that

$$p^*_{Y^n|h_1}(\mathcal{A}_n) \leq \exp(-nt). \tag{11}$$

The inequalities (9), (10), and (11) jointly lead to

$$\begin{aligned}\lim_{\varepsilon \to 1} \beta_s(n, \varepsilon) \leq & \exp(-nt) \\ \leq & \exp\left(-n \inf_{\gamma^n(s)} \left\{\frac{1}{n} \mathrm{D}(p_{Y^n|h_0} || p_{Y^n|h_1})\right\}\right),\end{aligned}$$

i.e., for all $n \in \mathbb{Z}_+$, we have

$$\lim_{\varepsilon \to 1} \frac{1}{n} \log \frac{1}{\beta_s(n, \varepsilon)} \geq \inf_{\gamma^n(s)} \left\{\frac{1}{n} \mathrm{D}(p_{Y^n|h_0} || p_{Y^n|h_1})\right\}.$$

In the asymptotic regime as $n \to \infty$, we have

$$\begin{aligned}&\lim_{\varepsilon \to 1} \liminf_{n \to \infty} \frac{1}{n} \log \frac{1}{\beta_s(n, \varepsilon)} \\ &\geq \lim_{n \to \infty} \inf_{\gamma^n(s)} \left\{\frac{1}{n} \mathrm{D}(p_{Y^n|h_0} || p_{Y^n|h_1})\right\} = \theta(s),\end{aligned}$$

where the last equality follows from Lemma 1. ∎

When ε is close to one, the bounds of the asymptotic exponential decay rate of the maximum minimal Type II probability of error are tight, which is made more concrete in the following corollary.

Corollary 1. *Given $s > 0$,*

$$\lim_{\varepsilon \to 1} \lim_{n \to \infty} \frac{1}{n} \log \frac{1}{\beta_s(n, \varepsilon)} = \theta(s).$$

Remark 1. *Given $s > 0$, letting $\varepsilon \to 1$ represents the worst privacy leakage scenario.*

In the following, we characterize the asymptotic performances of two special privacy-preserving energy management policies in the worst case scenario, i.e., $\varepsilon \to 1$.

IV. Asymptotic Characteristics of Special Privacy-Preserving Policies

A. Memoryless Hypothesis-Aware Policy

In practice, the EMU might have a limited processing capability, and at time slot i, applies a random memoryless hypothesis-aware energy management policy π_i to determine the energy supply y_i based on the current demand x_i and the hypothesis information h as

$$\pi_i : \mathcal{X} \times \mathcal{H} \to \mathcal{Y} | x_i - y_i \geq 0. \tag{12}$$

Let $\pi^n \triangleq \{\pi_i\}_{i=1}^n : \mathcal{X}^n \times \mathcal{H} \to \mathcal{Y}^n$ denote a memoryless hypothesis-aware energy management policy over an n-slot time horizon. If π^n satisfies the average energy constraint in (2), it is denoted by $\pi^n(s)$. When the EMU uses the optimal privacy-preserving memoryless hypothesis-aware policy, the achieved maximum minimal Type II probability of error subject to a Type I probability of error upper bound ε is denoted by

$$\beta_{\mathrm{L}}(n, \varepsilon, s) \triangleq \max_{\pi^n(s)} \{\beta(n, \varepsilon, \pi^n(s))\}. \tag{13}$$

We similarly define $\theta_{\mathrm{L}}(s)$ as

$$\theta_{\mathrm{L}}(s) \triangleq \inf_{k, \pi^k(s)} \left\{\frac{1}{k} \mathrm{D}(p_{Y^k|h_0} || p_{Y^k|h_1})\right\}. \tag{14}$$

The following corollary of Theorem 1 specifies the asymptotic exponential decay rate of the maximum minimal Type II probability of error by the divergence rate expression $\theta_{\mathrm{L}}(s)$ when the EMU uses the optimal privacy-preserving memoryless hypothesis-aware policy.

Corollary 2. *Given $s > 0$,*

$$\lim_{\varepsilon \to 1} \lim_{n \to \infty} \frac{1}{n} \log \frac{1}{\beta_{\mathrm{L}}(n, \varepsilon, s)} = \theta_{\mathrm{L}}(s). \tag{15}$$

We next show that the asymptotic exponential decay rate of the maximum minimal Type II probability of error can also be characterized by a single-letter divergence expression. Given $\bar{s}$, $\tilde{s} > 0$, we define $\phi(\bar{s}, \tilde{s})$ as

$$\phi(\bar{s}, \tilde{s}) \triangleq \min_{\substack{p_{Y|X,h_0} \\ p_{Y|X,h_1}}} \left\{\mathrm{D}(p_{Y|h_0} || p_{Y|h_1})\right\}, \quad \begin{array}{l} \mathrm{E}[X - Y|h_0] \leq \bar{s} \\ \mathrm{E}[X - Y|h_1] \leq \tilde{s} \\ p_{Y|X,h_0}(y|x) = 0, \text{ if } y > x \\ p_{Y|X,h_1}(y|x) = 0, \text{ if } y > x \end{array} \tag{16}$$

where $\mathrm{E}[X - Y|h_0] \leq \bar{s}$ denotes the single-slot average energy constraint under hypothesis h_0; $\mathrm{E}[X - Y|h_1] \leq \tilde{s}$ denotes the single-slot average energy constraint under hypothesis h_1; and $p_{Y|X,h_0}(y|x) = p_{Y|X,h_1}(y|x) = 0$ for all $y > x$ corresponds to the instantaneous constraint of the nonnegative energy supply from the RES at a single slot under both hypotheses.

Lemma 2. *$\phi(\bar{s}, \tilde{s})$ is a non-increasing, continuous, and convex function for $\bar{s} > 0$ and $\tilde{s} > 0$.*

The non-increasing property of $\phi(\bar{s}, \tilde{s})$ is self-evident. Its convexity follows from the convexity of $\mathrm{D}(\cdot||\cdot)$ and the definition of $\phi(\bar{s}, \tilde{s})$. The continuity of $\phi(\bar{s}, \tilde{s})$ follows from its convexity [20]. The complete proof is given in [16].

Theorem 2. *Given $s > 0$,*

$$\theta_{\mathrm{L}}(s) = \phi(s, s). \tag{17}$$

Proof: For any $k \in \mathbb{Z}_+$, $\pi^k(s)$, and the resulting $p_{Y^k|h_0}$, $p_{Y^k|h_1}$, we have

$$\begin{aligned}
&\frac{1}{k}\mathrm{D}\left(p_{Y^k|h_0}||p_{Y^k|h_1}\right)\\
&\overset{(a)}{=}\frac{1}{k}\sum_{i=1}^{k}\mathrm{D}\left(p_{Y_i|h_0}||p_{Y_i|h_1}\right)\\
&\overset{(b)}{\geq}\frac{1}{k}\sum_{i=1}^{k}\phi\left(\mathrm{E}[X_i-Y_i|h_0],\mathrm{E}[X_i-Y_i|h_1]\right)\\
&\overset{(c)}{\geq}\phi\left(\mathrm{E}\left[\frac{1}{k}\sum_{i=1}^{k}(X_i-Y_i|h_0)\right],\mathrm{E}\left[\frac{1}{k}\sum_{i=1}^{k}(X_i-Y_i|h_1)\right]\right)\\
&\overset{(d)}{\geq}\phi(s,s),
\end{aligned}$$

where (a) follows since the policy $\pi^k(s)$ leads to $p_{Y^k|h_j} = \prod_{i=1}^{k} p_{Y_i|h_j}$ for $j = 0, 1$; (b) follows from the definition of $\phi(\bar{s}, \tilde{s})$; (c) and (d) follow from the convexity and the non-increasing property of $\phi(\bar{s}, \tilde{s})$, respectively.

Therefore, we have

$$\theta_{\mathrm{L}}(s) = \inf_{k,\pi^k(s)}\left\{\frac{1}{k}\mathrm{D}(p_{Y^k|h_0}||p_{Y^k|h_1})\right\} \geq \phi(s,s). \tag{18}$$

The proof of the opposite direction is straightforward. Let $(p^*_{Y|X,h_0}, p^*_{Y|X,h_1})$ be the solution which achieves $\phi(s,s)$. It can be seen as a single-slot memoryless hypothesis-aware policy $\pi^1(s)$. From the definition of $\theta_{\mathrm{L}}(s)$ in (14), it follows that

$$\theta_{\mathrm{L}}(s) \leq \phi(s,s). \tag{19}$$

Alternatively, the inequality (19) follows since $\phi(s,s)$ is the asymptotic exponential decay rate of the minimal Type II probability of error achieved by a memoryless hypothesis-aware policy by using the single-slot policy $(p^*_{Y|X,h_0}, p^*_{Y|X,h_1})$ at all slots.

The inequalities (18) and (19) jointly lead to Theorem 2. ■

B. Hypothesis-Unaware Policy with Memory

We now consider the case when the EMU does not know the correct hypothesis but has a large memory storage and a powerful processing capability. At time slot i, the EMU follows a random hypothesis-unaware energy management policy with memory ρ_i to determine the energy supply y_i from the EP based on the demands x^i and the past supplies y^{i-1} as

$$\rho_i : \mathcal{X}^i \times \mathcal{Y}^{i-1} \to \mathcal{Y} | x_i - y_i \geq 0. \tag{20}$$

Let $\rho^n \triangleq \{\rho_i\}_{i=1}^n : \mathcal{X}^n \to \mathcal{Y}^n$ denote a hypothesis-unaware energy management policy with memory over an n-slot time horizon. If ρ^n satisfies the average energy constraint in (2), it is denoted by $\rho^n(s)$. When the EMU uses the optimal privacy-preserving hypothesis-unaware policy with memory, the achieved maximum minimal Type II probability of error subject to a Type I probability of error upper bound ε is denoted by

$$\beta_{\mathrm{M}}(n,\varepsilon,s) \triangleq \max_{\rho^n(s)}\{\beta(n,\varepsilon,\rho^n(s))\}. \tag{21}$$

We similarly define $\theta_{\mathrm{M}}(s)$ as

$$\theta_{\mathrm{M}}(s) \triangleq \inf_{k,\rho^k(s)}\left\{\frac{1}{k}\mathrm{D}(p_{Y^k|h_0}||p_{Y^k|h_1})\right\}. \tag{22}$$

As specified in the following corollary of Theorem 1, the asymptotic exponential decay rate of the maximum minimal Type II probability of error can be characterized by the divergence rate expression $\theta_{\mathrm{M}}(s)$ when the EMU uses the optimal privacy-preserving hypothesis-unaware policy with memory.

Corollary 3. *Given $s > 0$,*

$$\lim_{\varepsilon\to 1}\lim_{n\to\infty}\frac{1}{n}\log\frac{1}{\beta_{\mathrm{M}}(n,\varepsilon,s)} = \theta_{\mathrm{M}}(s). \tag{23}$$

Compared with the privacy-preserving memoryless hypothesis-aware policy, the privacy-preserving hypothesis-unaware policy with memory has all past demands and supplies while it does not know the correct hypothesis. We next compare the asymptotic privacy-preserving performances of the two policies.

Theorem 3. *Given $s > 0$,*

$$\theta_{\mathrm{M}}(s) \leq \phi(s,s). \tag{24}$$

The proof of Theorem 3 is presented in [16]. The proof idea is to show that a constructed two-phase hypothesis-unaware policy with memory can achieve the same asymptotic performance as the optimal privacy-preserving memoryless hypothesis-aware policy.

Remark 2. *The optimal privacy-preserving memoryless hypothesis-aware policy cannot outperform the optimal privacy-preserving hypothesis-unaware policy with memory. That is because the EMU having no direct access to the hypothesis information can learn the hypothesis with an arbitrarily small probability of error after observing a sufficiently long energy demand process.*

V. Asymptotic Privacy-Preserving Guarantee and Numerical Example

In Corollaries 1-3, we have characterized the asymptotic exponential decay rate of the maximum minimal Type II probability of error in the worst privacy leakage scenario by a divergence rate expression. However, the numerical evaluation of $\theta(s)$ or $\theta_{\mathrm{M}}(s)$ is difficult. On the other hand, $\phi(s,s)$ provides an upper bound on the optimal asymptotic exponential decay rate. Hence, we use the single-letter divergence expression $\phi(s,s)$ as an asymptotic privacy-preserving guarantee in this work.

While solving the optimization problem in (16) leads to the asymptotic privacy-preserving guarantee, the energy supply alphabet $\mathcal{Y}$ can be arbitrarily large which means a highly complex optimization problem. Moreover, the energy demand alphabet $\mathcal{X}$ is determined by a number of operation modes of the appliances and is typically finite. We show in the next

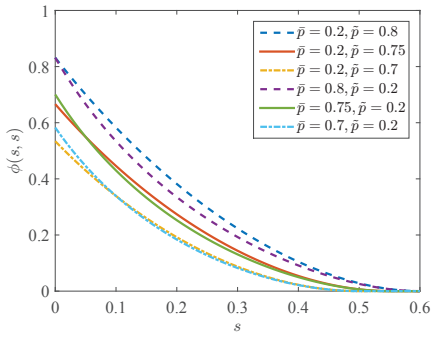

Fig. 2. Asymptotic privacy-preserving guarantee $\phi(s,s)$ for a binary demand model under different settings of $\bar{p}$, $\tilde{p}$.

theorem that the alphabet $\mathcal{Y}$ can be limited to the alphabet $\mathcal{X}$. This result can greatly simplify the numerical evaluation of the asymptotic privacy-preserving guarantee.

Theorem 4. *The energy supply alphabet can be limited to the energy demand alphabet under both hypotheses without loss of optimality.*

The proof of Theorem 4 can be found in [16]. It follows from the optimality in the definition of $\phi(s,s)$ and the data processing inequality of Kullback-Leibler divergence [21].

Here, we present a simple example with binary energy demands, i.e., $\mathcal{X}=\{0,1\}$. Based on Theorem 4, we only need to consider $\mathcal{Y}=\{0,1\}$. Denote $p_{X|h_0}(0)$ by $\bar{p}$ and $p_{X|h_1}(0)$ by $\tilde{p}$. The asymptotic privacy-preserving guarantee, $\phi(s,s)$, is shown in Fig. 2 for different values of $\bar{p}$ and $\tilde{p}$. Confirming the claim in Lemma 2, we observe that $\phi(s,s)$ is convex and non-increasing. When $s=0$, $x=y$ under both hypotheses and $\phi(0,0)=\mathrm{D}(p_{X|h_0}||p_{X|h_1})$. Intuitively, it is more difficult for the AD to identify the hypotheses when they lead to more similar energy demand profiles. It can be observed in Fig. 2 that $\phi(s,s)$ decreases as $\tilde{p}$ (resp. $\bar{p}$) gets closer to the fixed $\bar{p}$ (resp. $\tilde{p}$). Another interesting observation is that $\phi(s,s)$ curves for different settings of energy demand statistics $(\bar{p},\tilde{p})$ might intersect. This means that, to achieve a privacy-preserving guarantee, a lower RES average energy generation rate is required for $(\bar{p},\tilde{p})_{(\mathrm{A})}$ than that for $(\bar{p},\tilde{p})_{(\mathrm{B})}$; while to achieve anther privacy-preserving guarantee, a higher RES average energy generation rate is required for $(\bar{p},\tilde{p})_{(\mathrm{A})}$ than that for $(\bar{p},\tilde{p})_{(\mathrm{B})}$.

VI. Conclusion

We have modeled the smart meter privacy problem as a Neyman-Pearson test on the consumer behavior, and characterized different privacy-preserving energy management policies in the asymptotic regime by divergence rate expressions. In the worst case scenario where the Type I probability of error upper bound is close to one, we obtained a single-letter divergence expression for the asymptotic exponential decay rate of the maximum minimal Type II probability of error if the privacy-preserving memoryless hypothesis-aware policy is used; and we showed that the privacy-preserving memoryless hypothesis-aware policy cannot outperform the privacy-preserving hypothesis-unaware policy with memory. Furthermore, we have proved that the energy supply alphabet can be constrained to the energy demand alphabet without loss of optimality for the evaluation of the single-letter-divergence privacy-preserving guarantee, which can simplify the problem and the numerical simulation. More importantly, we have shown that the proposed two-phase hypothesis-unaware energy management policy with memory, where the EMU first learns the consumer behavior, can achieve the same asymptotic performance as the privacy-preserving memoryless hypothesis-aware policy.

References

[1] O. Tan, D. Gündüz, and H. V. Poor, "Increasing smart meter privacy through energy harvesting and storage devices," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1331–1341, 2013.

[2] F. Sultanem, "Using appliance signatures for monitoring residential loads at meter panel level," *IEEE Transactions on Power Delivery*, vol. 6, no. 4, pp. 1380–1385, 1991.

[3] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*, 2010, pp. 61–66.

[4] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Proceedings of SmartGridComm 2010*, 2010, pp. 327–332.

[5] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Proceedings of SmartGridComm 2010*, 2010, pp. 232–237.

[6] D. Varodayan and A. Khisti, "Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage," in *Proceedings of ICASSP 2011*, 2011, pp. 1932–1935.

[7] D. Gündüz and J. Gómez-Vilardebó, "Smart meter privacy in the presence of an alternative energy source," in *Proceedings of ICC 2013*, 2013, pp. 2027–2031.

[8] Z. Li and T. J. Oechtering, "Privacy on hypothesis testing in smart grids," in *Proceedings of ITW 2015 Fall*, 2015, pp. 337–341.

[9] G. Giaconi, D. Gündüz, and H. V. Poor, "Smart meter privacy with an energy harvesting device and instantaneous power constraints," in *Proceedings of ICC 2015*, 2015, pp. 7216–7221.

[10] L. Willenborg and T. d. Waal, *Elements of Statistical Disclosure Control*. Springer-Verlag New York, 2001.

[11] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, "Local privacy and statistical minimax rates," in *Proceedings of FOCS 2013*, 2013, pp. 429–438.

[12] Z. Li and T. J. Oechtering, "Privacy-aware distributed Bayesian detection," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 7, pp. 1345–1357, 2015.

[13] B. Tondi, M. Barni, and N. Merhav, "Detection games with a fully active attacker," in *Proceedings of WIFS 2015*, 2015, pp. 1–6.

[14] J. Liao, L. Sankar, V. Y. F. Tan, and F. P. Calmon, "Hypothesis testing in the high privacy limit," in *Proceedings of Allerton 2016*, 2016, pp. 649–656.

[15] ——, "Hypothesis testing under mutual information privacy constraints in the high privacy regime," eprint arXiv:1704.08347.

[16] Z. Li, T. J. Oechtering, and D. Gündüz, "Smart meter privacy: Adversarial hypothesis testing models," in preparation.

[17] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press, 2011.

[18] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley-Interscience, 1991.

[19] T. S. Han, *Information-Spectrum Methods in Information Theory*. Springer Berlin Heidelberg, 2003.

[20] "Every convex function is locally Lipschitz," *The American Mathematical Monthly*, vol. 79, no. 10, pp. 1121–1124, 1972.

[21] T. van Erven and P. Harremoës, "Rényi divergence and Kullback-Leibler divergence," *IEEE Transactions on Information Theory*, vol. 60, no. 7, pp. 3797–3820, 2014.