KTH Electrical Engineering

Privacy-by-Design for Cyber-Physical Systems

ZUXING LI

Doctoral Thesis in Electrical Engineering
Stockholm, Sweden 2017

Department of Information Science and Engineering
KTH, School of Electrical Engineering
SE-100 44 Stockholm
SWEDEN

TRITA-EE 2017:057
ISSN 1653-5146
ISBN 978-91-7729-458-0

Akademisk avhandling som med tillstånd av Kungl Tekniska högskolan framlägges till offentlig granskning för avläggande av teknologie doktorsexamen i Elektroteknik onsdag den 13 september 2017 klockan 13.15 i F3, Lindstedtsvägen 26, Stockholm.

Tryck: Universitetsservice US AB

To my beloved sister

Abstract

It is envisioned that future cyber-physical systems will provide a more convenient living and working environment. However, such systems need inevitably to collect and process privacy-sensitive information. That means the benefits come with potential privacy leakage risks. Nowadays, this privacy issue receives more attention as a legal requirement of the EU General Data Protection Regulation. In this thesis, privacy-by-design approaches are studied where privacy enhancement is realized through taking privacy into account in the physical layer design. This work focuses in particular on cyber-physical systems namely sensor networks and smart grids. Physical-layer performance and privacy leakage risk are assessed by hypothesis testing measures.

First, a sensor network in the presence of an informed eavesdropper is considered. Extended from the traditional hypothesis testing problems, novel privacy-preserving distributed hypothesis testing problems are formulated. The optimality of deterministic likelihood-based test is discussed. It is shown that the optimality of deterministic likelihood-based test does not always hold for an intercepted remote decision maker and an optimal randomized decision strategy is completely characterized by the privacy-preserving condition. These characteristics are helpful to simplify the person-by-person optimization algorithms to design optimal privacy-preserving hypothesis testing networks.

Smart meter privacy becomes a significant issue in the development of smart grid technology. An innovative scheme is to exploit renewable energy supplies or an energy storage at a consumer to manipulate meter readings from actual energy demands to enhance the privacy. Based on proposed asymptotic hypothesis testing measures of privacy leakage, it is shown that the optimal privacy-preserving performance can be characterized by a Kullback-Leibler divergence rate or a Chernoff information rate in the presence of renewable energy supplies. When an energy storage is used, its finite capacity introduces memory in the smart meter system. It is shown that the design of an optimal energy management policy can be cast to a belief state Markov decision process framework.

Sammanfattning

Framtidens cyberfysiska system förväntas resultera i bekvämare levnads- och arbetsmiljö för många människor. Sådana system behöver emellertid ofrånkomligen samla och behandla sekretesskänslig information. Detta för med sig risker kopplade till integritet. På senare tid har denna sekretessfråga fått mer uppmärksamhet till följd av ett rättsligt krav i EU:s allmänna dataskyddsförordning. I denna avhandling studeras strategier för privacy-by-design, där integritetsförbättringar realiseras genom att ta hänsyn till sekretess i den fysiska algoritmdesignen. Särskilt fokus läggs på cyberfysiska system, såsom sensornätverk och smarta nät. Prestandan hos algoritmdesignen och risken för integritetskränkningar utvärderas med hjälp av hypotesprövning.

Inledningsvis studeras ett sensornätverk i en omgivning med en informerad tjuvlyssnare. Nya integritetsbevarande distribuerade hypotesprövningsproblem formuleras som utvidgningar av traditionella hypotesprövningsproblem. Optimaliteten av det deterministiska likelihood-baserade testet diskuteras. Det visas att det deterministiska likelihood-baserade testet inte alltid håller för en avlägsen avlyssnad beslutsfattare, och att en optimal stokastisk beslutsstrategi är fullständigt definierad av det integritetsbevarande villkoret. Dessa attribut hjälper till att förenkla person-by-person-optimeringsalgoritmer för att designa optimala integritetsbevarande nätverk för hypotesprövning.

Integriteten hos smartmätare kommer att vara en viktig fråga under teknikutvecklingen för smarta nät. En idé är att utnyttja energi lagrad hos en konsument för att manipulera mätvärden av de faktiska energibehoven, och därmed förbättra integriteten. Baserat på föreslagna asymptotiska hypotesprövningsmått av sekretessläckage visas det att den optimala integritetsbevarande prestandan kan karakteriseras av en Kullback-Leibler-divergence rate eller en Chernoff-information rate i närvaro av lager av förnyelsebar energi. När ett energilager förbrukas, introducerar dess ändliga kapacitet minne i smartmätarsystemet. Det visas att utformningen av en optimal energihanteringspolicy kan formulas som en belief state Markov decision process.

Acknowledgements

This thesis could not be finished without the help and support from many professors, colleagues, friends, and my family. It is my pleasure to acknowledge people who give me help, guidance, and encouragement.

First and foremost, I would like to thank my main supervisor Assoc. Prof. Tobias Oechtering. You offer me the opportunity to pursue Ph.D. degree, always provide me strong support and helpful guidance in the research, and share me positive philosophy.

I am deeply grateful to my co-supervisor Assoc. Prof. Joakim Jaldén for the valuable discussions in the DeWiNe group meetings. I would like to thank Assoc. Prof. Deniz Gündüz for hosting my visit of ICL and supervising my research in the COPES project.

I would like to express my sincere gratitude to Assoc. Prof. Stefano Marano from University of Salerno for acting as the opponent, and to the grading board members: Assoc. Prof. Edith Ngai from Uppsala University, Assoc. Prof. Aikaterini Mitrokotsa from Chalmers University of Technology, Assoc. Prof. Pablo Piantanida from Supelec Télécom, and Prof. Mats Bengtsson. I would like to thank Prof. Mikael Skoglund for being the defense chair and Prof. Magnus Jansson for advance thesis review.

I must thank all my colleagues for creating the enjoyable working environment. I would like to thank Dr. Kittipong Kittichokechai for supervising my master thesis project and helping me in the beginning of my Ph.D. study. I feel grateful to work with the seniors: Prof. Peter Händel, Prof. Lars Kildehøj, Assoc. Prof. Ming Xiao, Assoc. Prof. Ragnar Thobaben, Assoc. Prof. James Gross, Assoc. Prof. Markus Flierl, Assis. Prof. Saikat Chatterjee, Dr. Satyam Dwivedi, Dr. Isaac Skog, Dr. Jinfeng Du, Dr. Ali Zaidi, Dr. Hieu Do, Dr. Ricardo Blasco Serrano, Dr. Mattias Andersson, Dr. Jalil Taghia, Dr. Amirpasha Shirazinia, Dr. Dennis Sundman, Dr. Frédéric Gabry, Dr. Hamed Farhadi, Dr. Maksym Girnyk, Dr. Iqbal Hussain, Dr. Sheng Huang, Dr. Zhao Wang, Dr. Efthymios Stathakis, Dr. Tai Do, Dr. Haopeng Li, Dr. Leefke Grosjean, Dr. Hadi Ghauch, Dr. Majid Gerami, Dr. Alla Tarighati, Dr. Nima Najari Moghadam, Dr. Hussein Mohammed Al Zubaidy, Dr. Germán Bassi, Dr. Rami Mochaourab, Dr. Antonios Pitarokoilis, Dr. Qiwen Wang, Mr. Peter Larsson, and Mr. Ahti Ainomäe. I devote special thanks to Ms. Raine Tiivel, Ms. Dora Söderberg, and Ms. Tove Schwartz for careful and efficient

administrative support.

It is a pleasure to share the office with my talented officemate Minh Thanh Vu. I really enjoy the relaxed lunch time with Guang Yang, Bing Li, Nan Qi, Le Phuong Cao, Dr. Lin Zhang, Yu Ye, Zhengquan Zhang, Dong Liu, and Shaocheng Huang. I am grateful to have Marie Maros as my teaching partner, and to have Pol del Aguila Pla, Arash Owrang, Håkan Carlsson as my candy corner partners. It is my pleasure to have the nice fellows: C V Ramana Reddy Avula, Baptiste Cavarec, Hasan Basri Celebi, Henrik Forssell, Jin Huang, Xinyue Liang, Sahar Imtiaz, Robin Larsson Nordström, Du Liu, Nan Li, Alireza Mahdavi Javid, Sina Molavipour, Boules Atef Mouris, Sebastian Schiessl, Arun Venkitaraman, Johan Wahlström, and Hanwei Wu.

I am always indebted to my master study adviser Prof. Miguel Ángel Lagunas in UPC for encouraging me to do Ph.D. research. I would like to express my sincere gratitude to all professors who taught me during my master study in UPC and KTH. I would like to thank the master program assistant Ms. Lise Vierning for her Catalan warmth.

Finally, I would like to express my gratitude to my parents, my elder brother, and my precious sister for their love and support.

Zuxing Li
Stockholm, July 2017

Contents

Acronyms and Notations

Acronyms

AD	adversary
CPS	cyber-physical system
EMU	energy management unit
EP	energy provider
ES	energy storage
EVE	eavesdropper
FC	fusion center
GDPR	General Data Protection Regulation
i.i.d.	identically independently distributed
KKT	Karush-Kuhn-Tucker
LRC	likelihood-ratio chain
LRT	likelihood-ratio test
MDP	Markov decision process
p.d.f.	probability density function
p.m.f.	probability mass function
PBPO	person-by-person optimization
RES	renewable energy source
ROC	receiver operating characteristic

Notations

X	random variable
x	realization of the random variable X
$\mathcal{X}$	alphabet of the random variable X
X_i^k	random sequence $(X_i, \ldots, X_k)$
x_i^k	realization of the random sequence X_i^k
$\mathcal{X}_i^k$	alphabet of the random sequence X_i^k
X^k	random sequence $(X_1, \ldots, X_k)$
x^k	realization of the random sequence X^k
$\mathcal{X}^k$	alphabet of the random sequence X^k
$X_i^{k\setminus n}$	random sequence $(X_i, \ldots, X_{n-1}, X_{n+1}, \ldots, X_k)$
$x_i^{k\setminus n}$	realization of the random sequence $X_i^{k\setminus n}$
$\mathcal{X}_i^{k\setminus n}$	alphabet of the random sequence $X_i^{k\setminus n}$
$X^{k\setminus n}$	random sequence $(X_1, \ldots, X_{n-1}, X_{n+1}, \ldots, X_k)$
$x^{k\setminus n}$	realization of the random sequence $X^{k\setminus n}$
$\mathcal{X}^{k\setminus n}$	alphabet of the random sequence $X^{k\setminus n}$
$\|\| \cdot \|\|$	set cardinality
f_X	p.d.f. of the continuous random variable X
p_X	p.m.f. of the discrete random variable X
$\mathcal{N}(\mu, \sigma^2)$	normal distribution with mean μ and variance σ^2
$\mathrm{D}(\cdot\|\|\cdot)$	Kullback-Leibler divergence
$\mathrm{D}_\tau(\cdot\|\|\cdot)$	τ-th order Rényi divergence
$\mathrm{C}(\cdot, \cdot)$	Chernoff information
$\mathrm{E}[\cdot]$	expectation
$\partial\cdot$	boundary of a closed set

$\hat{\partial}\cdot$	upper boundary of a two-dimensional closed set
$\check{\partial}\cdot$	lower boundary of a two-dimensional closed set
$\log(\cdot)$	natural logarithm

Chapter 1

Introduction

1.1 Privacy Challenge in Cyber-Physical System

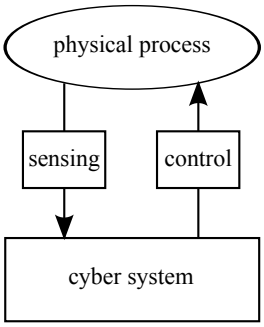


Figure 1.1: Illustration of a CPS.

A cyber-physical system (CPS) consists of two major components: a physical process and a cyber system. As shown in Figure 1.1, the physical process, which can be a natural phenomenon or a man-made physical system, is monitored and controlled by the cyber system, which typically is a networked system of several tiny devices with sensing, computation, and communication capabilities [62]. There have been a large number of proposed CPS applications, such as smart house, smart grid, eHealth, assisted living, and etc. They are envisioned to form a smart environment which will greatly benefit the users. A typical CPS often collects a huge amount of privacy-sensitive information for data analysis and decision making. The information enables the system to make smart decisions through sophisticated algorithms. However, a privacy leakage could potentially happen in any stage(s) of data collection, data transmission, data processing, or data storage. On the other hand, there is an increasing demand to protect privacy, e.g., the EU General Data Protection Regulation (GDPR) [1] is to replace the Data Protection Directive

95/46/EC and is designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy, and to reshape the way organizations across the region approach data privacy. Therefore, research on privacy protection for CPSs attracts much attention nowadays. In the next, researches on privacy protection are briefly reviewed.

1.2 Literature Review

In face of a variety of privacy threats, a large amount of fruitful works have been done. As a conventional privacy-preserving tool, cryptography was reported in many papers, e.g., [50], to protect the private data. Although it is an effective method, cryptography is not always applicable because of its demands of high computation capability, high power consumption, and complicated key management. Some studies investigated the privacy-protection in the multi-hop routing, e.g., the reputation-based scheme [9] and the broadcast authentication [42].

All these aforementioned technologies use additive privacy functionality blocks and cannot protect privacy against the authorized data recipient. GDPR calls for an authorized data recipient to hold and process only the data absolutely necessary for the completion of its duties as well as limiting the access to personal data to those needing to act out the processing [1]. To this end, GDPR advocates the *privacy-by-design* approach which can "inherently" preserve privacy through the inclusion of data protection from the onset of the designing of systems rather than an addition afterward. Depending on the physical-layer operations, privacy-by-design approaches can further be categorized into different classes.

Until now, most privacy-by-design approaches focus on the data transmission stage, which corresponds to sensing and communication in the physical layer of a CPS. The study on the wire-tap channel [63] derives the secrecy capacity. Based on the theory of wire-tap channel, people have developed privacy schemes, such as artificial noise [16] and cooperative jamming [56]. Recently, secure data compression in source coding also attracts much attention [26].

Besides data transmission, there are other physical-layer operations for a CPS application. Consider the eHealth system in Figure 1.2 which consists of wearable or embedded sensors and a handheld terminal. The sensors collect different raw data, e.g., heart rate, body temperature, or blood pressure, process the raw data to make sensor decisions, and then transmit the sensor decisions to the terminal. The terminal makes the final conclusion of the user health condition based on the received sensor decisions. This eHealth CPS operation can be seen as a statistical inference on the user health condition through a sensor network. The statistical inference operation in the physical layer can be modeled as a *hypothesis test*[1] or an estimation.

[1]Note that there are other terms, e.g., *detection* and *classification*, used to refer to a hypothesis test in many literatures.

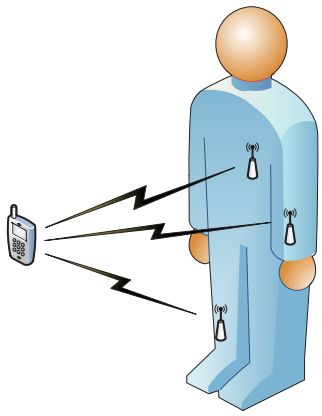


Figure 1.2: Illustration of an eHealth network which consists of tiny sensors and a terminal.

A statistical inference can be done centrally or distributively. The corresponding hypothesis testing theorems have been well established. A brief introduction of the centralized hypothesis testing problems based on the Bayesian approach and Neyman-Pearson approach was presented in [59]. In [57, 61], the basic distributed hypothesis testing problems were summarized of different formulations, topologies, processing and communication constraints. Extended distributed hypothesis testing problems were reviewed in [7].

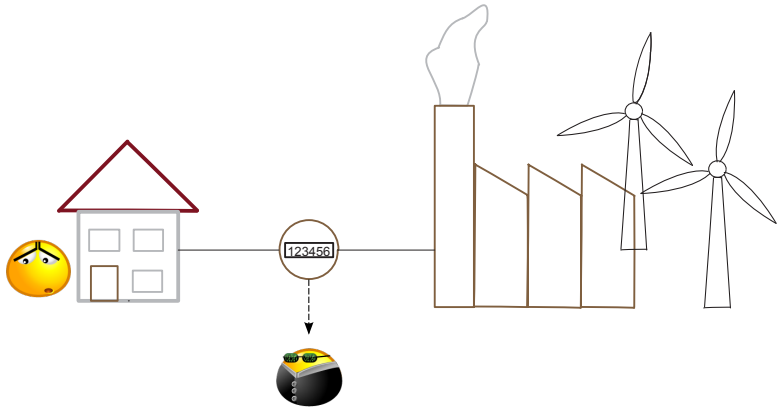
When the privacy-by-design approach is used, the privacy-preserving objective is taken into account in the hypothesis tests and the established hypothesis testing theorems need to be revised. There are two pioneering works [43, 47] which considered a distributed hypothesis testing network in the presence of an eavesdropper. In [43], the eavesdropper is assumed to be only interested in the data transmission state between the remote decision makers and the fusion center. However, an eavesdropper in reality can be more aggressive and tries to intercept the transmitted information for malicious purposes. When the eavesdropper makes a hypothesis test based on the intercepted decisions of remote decision makers, it has been shown in [47] that a likelihood-ratio test (LRT) is an asymptotically optimal decision strategy of a remote decision maker under a constraint on the eavesdropping performance measured by a Kullback-Leibler divergence. Whereas, it was not provided how to design the asymptotically optimal privacy-preserving distributed hypothesis testing network. A recent work [44] characterized an achievable rate-error-equivocation region of a distributed hypothesis testing network with communication and privacy constraints. Unfortunately, the converse proof was only given for a special case. Some works devised privacy schemes based on the assumption that the eavesdropper is uninformed of certain parameters. In [46, 53], they

studied stochastic encryption methods where remote decision makers intentionally generate error to confuse the eavesdropper which is uninformed of the error statistics. Similarly, works [21,22] proposed channel aware encryption methods to design the transmission scheme between the remote decision makers and the fusion center based on the channel states which are not known by the eavesdropper.

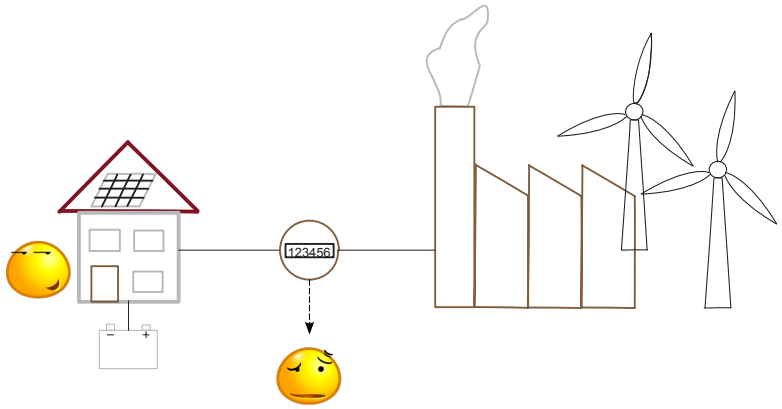
The privacy issue is also addressed in a distributed estimation context. Some works used a similar method of stochastic encryption, e.g., a stochastic cipher was utilized in [3] to protect privacy in a network where both the fusion center and eavesdropper make maximum-likelihood estimations. In [18], the optimal power allocation scheme was studied in a decentralized minimum mean square error estimation susceptible to eavesdropping.

In the aforementioned privacy-by-designs of statistical inference operation in the physical layer, the privacy leakage can also be modeled as a statistical inference made by an eavesdropper or adversary. Besides hypothesis test and estimation, the statistical inference risks have been discussed and evaluated in computer science through the differential privacy. Differential privacy [14] was proposed to guarantee the statistical privacy by sanitizing mechanisms when an adversary has access to two neighbor databases. In [24], the degradation of the differential privacy level under adaptive interactions was characterized. In [52], for any statistical estimator and input distribution satisfying a regularity condition, it was proved that there exists a differentially private estimator with the same asymptotic output distribution. In [28], the methods were developed to approximate a filter by its differentially private version. A survey of the differential privacy in machine learning was given in [23]. Relations between different formalisms for statistical inference privacy were discussed in [4].

Smart grid is one of the most attractive CPS applications. Real-time information about energy demands and advanced control and communication technologies enable more efficient energy generation and distribution in smart grids [55]. Real-time energy demand information is provided to the energy provider 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 [45,54]. A number of privacy-preserving technologies have been developed for the smart meter privacy problem in the recent years. In [29], an encryption method was proposed to protect the privacy of an individual consumer through data aggregation in the neighborhood. In [25], a privacy scheme was devised by scheduling delay-tolerable appliances to hide the energy demand profiles of others. Most of the literature focuses on the manipulation of meter readings to preserve privacy, e.g., adding a noise sequence on the meter readings. There is a growing interest in guaranteeing privacy by directly altering the energy demands from the energy provider. This can be achieved by an energy management of renewable energy supplies or energy storage charge/discharge flows to filter the real energy demand characteristics. Information-theoretic approaches to these problems have been studied in [15, 17, 55, 60]. In these works, the privacy leakage measure is the mutual information rate between the energy demand sequence and the energy



(a)



(b)

Figure 1.3: Illustration of the smart meter privacy problem and the privacy-by-design approach which exploits renewable energy supplies or an energy storage.

supply sequence. The information-theoretic measure can be adopted regardless of the real adversary behavior. However, it lacks an operational meaning. An optimal privacy-preserving energy management of the renewable energy supply or the energy storage charge/discharge is designed to minimize the mutual information rate. Based on the observation that a constant meter reading sequence does not leak any privacy, another privacy-preserving idea was proposed in [64] to utilize an energy storage to minimize the variance of random energy supplies from the energy provider. Similar to the information-theoretic privacy leakage measure, a variance does not have a clear operational meaning. Recently, a hypothesis testing measure of smart meter privacy was proposed in [35] and the discussion of a privacy-

preserving energy management was based on an infinite-capacity energy storage. The hypothesis testing measure has a clear operational meaning while it limits the adversary behavior to be a hypothesis test. System memory is commonly inevitable in the energy management problems, e.g., the utilization of a finite-capacity energy storage. In [30, 65, 66], a privacy-preserving energy management in the presence of an energy storage was cast to a Markov decision process framework.

1.3 Thesis Outline

The general research question of this work is *how to realize privacy-preserving CPSs*. In this thesis, the privacy-by-design approaches are investigated in the contexts of a distributed sensor network and a smart meter system. The sensing data or the energy data processed in the CPS is driven by a privacy-sensitive unknown physical process, e.g., health condition or life style of the user. A such unknown physical process can be seen as a hypothesis. In this work, hypothesis tests are assumed for the physical-layer operation of a CPS and the privacy leakage. The following questions are to be discussed in the remaining chapters:

- *How to measure the privacy leakage?*
- *Does the optimality of deterministic likelihood-based test (or LRT) hold when the privacy is taken into account?*
- *What are the optimality characteristics if a randomized strategy is needed?*
- *How to design an optimal privacy-preserving network?*
- *How to characterize an optimal privacy-preserving performance (bound)?*

Chapter 2

In this chapter, the basics of hypothesis tests are recapitulated. The Bayesian and Neyman-Pearson hypothesis testing approaches are introduced. The optimality of deterministic likelihood-based test (or LRT) is testified in centralized and distributed hypothesis tests by using the analysis tools of hypothesis testing operation region and person-by-person optimality argument. Depending on the hypothesis testing approach, it is shown that the asymptotic hypothesis testing performance can be characterized by a Kullback-Leibler divergence or a Chernoff information.

Chapter 3

In this chapter, optimal privacy-preserving designs of a distributed hypothesis testing network are characterized when Bayesian hypothesis testing performance and privacy leakage measures are used. With the tools of person-by-person optimality argument and hypothesis testing operation region, the optimality of deterministic

likelihood-based test (or LRT) is discussed. When an optimal randomized decision strategy is needed, it is determined by the privacy-preserving condition only. Based on the optimality characteristics, extended person-by-person optimization algorithms are proposed to design optimal privacy-preserving networks. The chapter content is based on

[34] Z. Li and T. J. Oechtering. Privacy-aware distributed Bayesian detection. *IEEE Journal of Selected Topics in Signal Processing*, 9(7):1345-1357, 2015.

Chapter 4

In this chapter, an optimal privacy-preserving design of a distributed binary hypothesis testing network is characterized when Neyman-Pearson hypothesis testing performance and privacy leakage measures are used. The optimality of deterministic LRT is shown to hold for the remote decision strategies when the same Neyman-Pearson testing constraints are used. The materials in this chapter are published in the following paper

[36] Z. Li and T. J. Oechtering. Privacy-constrained parallel distributed Neyman-Pearson test. *IEEE Transactions on Signal and Information Processing over Networks*, 3(1):77-90, 2017.

Chapter 5

In this chapter, the research on the optimal privacy-preserving energy management of an ideal renewable energy source is made with the tools of large deviation theory and information theory. The research focuses on the asymptotic privacy-preserving performance bounds. Under adversarial Neyman-Pearson and Bayesian hypothesis testing privacy leakages, it is shown that the asymptotic optimal privacy-preserving performances can be characterized by a Kullback-Leibler divergence rate and a Chernoff information rate, respectively; a single-letter Kullback-Leibler divergence and a single-letter Chernoff information are further shown to characterize the asymptotic optimal privacy-preserving performances of memoryless hypothesis-aware policy. This chapter is based on the following papers

[37] Z. Li, T. J. Oechtering, and D. Gündüz. Smart meter privacy: Adversarial hypothesis testing models. In Preparation for IEEE Transactions on Information Forensics and Security.

[38] Z. Li, T. J. Oechtering, and D. Gündüz. Smart meter privacy based on adversarial hypothesis testing. Accepted at ISIT 2017.

Chapter 6

In this chapter, the research on the optimal privacy-preserving energy management of a finite-capacity energy storage is made with the tool of Markov decision process.

It is shown that the optimization problem of energy management policies can be reformulated as a belief state Markov decision process problem. This chapter is based on

[41] Z. Li, T. J. Oechtering, and M. Skoglund. Privacy-preserving energy flow control in smart grids. In *Proceedings of ICASSP 2016*, pages 2194-2198, 2016.

Chapter 7

The conclusion is made in the final chapter: summary of main results presented in this thesis, possible future works, and significances of this work.

Related publications

The following publications are not covered in this thesis but contain related materials and applications.

[31] Z. Li and T. J. Oechtering. Differential privacy in parallel distributed Bayesian detections. In *Proceedings of Fusion 2014*, pages 1-7, 2014.

[32] Z. Li and T. J. Oechtering. Privacy-concerned parallel distributed Bayesian sequential detection. In *Proceedings of GlobalSIP 2014*, pages 928-932, 2014.

[33] Z. Li and T. J. Oechtering. Tandem distributed Bayesian detection with privacy constraints. In *Proceedings of ICASSP 2014*, pages 8168-8172, 2014.

[35] Z. Li and T. J. Oechtering. Privacy on hypothesis testing in smart grids. In *Proceedings of ITW 2015 Fall*, pages 337-341, 2015.

[39] Z. Li, T. J. Oechtering, and J. Jaldén. Parallel distributed Neyman-Pearson detection with privacy constraints. In *Proceedings of ICC 2014 Workshop*, pages 765-770, 2014.

[40] Z. Li, T. J. Oechtering, and K. Kittichokechai. Parallel distributed Bayesian detection with privacy constraints. In *Proceedings of ICC 2014*, pages 2178-2183, 2014.

[67] Y. You, Z. Li, and T. J. Oechtering. An optimal privacy-enhancing and cost-efficient energy management strategy. Submitted to WIFS 2017.

Chapter 2

Hypothesis Testing Problems

In this chapter, a recapitulation of the hypothesis testing problems is made. The presented results and theorems from the previous works serve as the fundamentals of discussions in the next chapters.

2.1 Bayesian and Neyman-Pearson Approaches

A centralized hypothesis testing scenario is described as follows: There is a binary hypothesis H which can take the value 0 or 1; a continuous random observation Y is generated conditioned on hypothesis 0 following a probability density function (p.d.f.) $f_{Y|H}(\cdot|0)$ or on hypothesis 1 following a p.d.f. $f_{Y|H}(\cdot|1)$; and a binary decision $\hat{H}$ is made based on the random observation Y and following a (randomized) hypothesis testing strategy $\phi : \mathcal{Y} \to \{0, 1\}$ to infer the correct hypothesis.

The p.d.f.s $f_{Y|H}(\cdot|0)$ and $f_{Y|H}(\cdot|1)$ are conventionally known as the observation likelihoods. The following assumption on a continuous random observation is commonly used in the binary hypothesis testing problems.

Assumption 2.1. *Given a continuous random observation Y, it is assumed that*

1. *Y has the same support set conditioned on different hypotheses;*
2. *The likelihoods $f_{Y|H}(\cdot|0)$ and $f_{Y|H}(\cdot|1)$ contain no point masses of probability;*
3. *The likelihood ratio $\frac{f_{Y|H}(\cdot|0)}{f_{Y|H}(\cdot|1)}$ contains no point masses of probability;*
4. *For all $0 \leq \lambda \leq 1$, there exist a non-negative value ρ and a corresponding set $\mathcal{A}(\rho) = \left\{ y \,\middle|\, \frac{f_{Y|H}(y|0)}{f_{Y|H}(y|1)} \geq \frac{1}{\rho} \right\}$ such that*

$$\int_{\mathcal{A}^c(\rho)} f_{Y|H}\left(y|0\right) dy = \lambda.$$

A hypothesis testing problem is to design a strategy which achieves the optimal hypothesis testing performance. In this work, Bayesian and Neyman-Pearson hypothesis testing approaches are used. In the following, the basics of the two hypothesis testing problems are illustrated in the context of the described centralized hypothesis testing scenario.

Bayesian hypothesis test

In a Bayesian hypothesis test, the hypothesis testing performance achieved by a strategy ϕ is measured by the Bayesian risk $r(\phi)$, which is defined as the expected decision cost as

$$r(\phi) = \mathrm{E}\left[c(\hat{H}, H)\right] = \int_{\mathcal{Y}} \sum_{\hat{h},h\in\{0,1\}} p_{\hat{H}|Y}(\hat{h}|y) f_{Y|H}(y|h) p_H(h) c(\hat{h}, h) dy, \tag{2.1}$$

where the conditional probability mass function (p.m.f.) $p_{\hat{H}|Y}$ alternatively represents the used strategy ϕ; the p.m.f. p_H denotes the prior probability distribution of the hypothesis; and $c(\hat{h}, h)$ denotes the cost of making a decision $\hat{h}$ when the correct hypothesis is h. The design objective of the (randomized) hypothesis testing strategy is to minimize the Bayesian risk

$$\phi^* = \arg\min_{\phi\in\Phi} r(\phi), \tag{2.2}$$

where Φ denotes the set of all feasible hypothesis testing strategies.

To minimize the Bayesian risk, given any observation $Y = y$, the decision of an optimal strategy ϕ^* is

$$\hat{H} = \phi^*(y) = \arg\min_{\hat{h}\in\{0,1\}} \sum_{h\in\{0,1\}} f_{Y|H}(y|h) p_H(h) c(\hat{h}, h). \tag{2.3}$$

The minimal Bayesian risk is

$$r(\phi^*) = \int_{\mathcal{Y}} \min_{\hat{h}\in\{0,1\}} \left\{ \sum_{h\in\{0,1\}} f_{Y|H}(y|h) p_H(h) c(\hat{h}, h) \right\} dy. \tag{2.4}$$

Under an assumption that a cost of making a correct decision is always smaller than a cost of making an incorrect decision, an optimal Bayesian hypothesis testing strategy can be equivalently specified as a deterministic LRT:

$$\hat{H} = \phi^*(y) = \begin{cases} 0, & \text{if } \dfrac{f_{Y|H}(y|0)}{f_{Y|H}(y|1)} \geq \dfrac{p_H(1)(c(0,1) - c(1,1))}{p_H(0)(c(1,0) - c(0,0))} \\ 1, & \text{otherwise} \end{cases}. \tag{2.5}$$

Remark 2.1. *In the considered centralized hypothesis testing scenario, a deterministic optimal strategy is identified. However, it is not necessary to have a unique and deterministic optimal strategy in a Bayesian hypothesis test, i.e., it is sufficient to consider the deterministic likelihood-based test in (2.3) for an optimal strategy of the Bayesian hypothesis test (2.2).*

Remark 2.2. *Given an arbitrary decision cost assignment, an optimal strategy of the Bayesian hypothesis test (2.2) may be a deterministic LRT with inversed decision regions of (2.5). For instance, if a cost of making a correct decision is always larger than a cost of making an incorrect decision, an optimal Bayesian hypothesis testing strategy can be equivalently specified as the following deterministic LRT:*

$$\hat{H} = \phi^*(y) = \begin{cases} 0, & \text{if } \dfrac{f_{Y|H}(y|0)}{f_{Y|H}(y|1)} \leq \dfrac{p_H(1)(c(0,1)-c(1,1))}{p_H(0)(c(1,0)-c(0,0))} \\ 1, & \text{otherwise} \end{cases}.$$

Remark 2.3. *Given $m > 2$, if an m-ary hypothesis is considered, it is sufficient to consider a deterministic likelihood-based test in the form of (2.3) for an optimal Bayesian hypothesis testing strategy.*

Neyman-Pearson hypothesis test

In a Bayesian hypothesis test, the prior probability distribution p_H needs to be known and the decision costs $\left\{c(\hat{h},h)\right\}_{\hat{h},h\in\{0,1\}}$ need to be defined beforehand. However, these parameters might not be available so that a Bayesian hypothesis test cannot be formulated. Instead, a Neyman-Pearson hypothesis test does not need these parameters.

In the considered centralized hypothesis testing scenario, a binary decision $\hat{H}$ is made to infer the binary hypothesis H. A strategy ϕ can be represented by the conditional p.m.f. $p_{\hat{H}|Y}$. Jointly with the likelihoods of the observation $f_{Y|H}(\cdot|0)$ and $f_{Y|H}(\cdot|1)$, the strategy ϕ can be alternatively represented by four types of conditional probabilities $\left\{p_{\hat{H}|H}(\hat{h}|h)\right\}_{\hat{h},h\in\{0,1\}}$, where

$$p_{\hat{H}|H}(\hat{h}|h) = \int_{\mathcal{Y}} p_{\hat{H}|Y}(\hat{h}|y) f_{Y|H}(y|h)dy. \tag{2.6}$$

Conventionally,

- $p_{\hat{H}|H}(1|0)$ is called the *false-alarm probability* (denoted by $p_{\mathrm{F}}(\phi)$) or the *Type I probability of error*;
- $p_{\hat{H}|H}(0|1)$ is called the *miss probability* (denoted by $p_{\mathrm{M}}(\phi)$) or the *Type II probability of error*;

- $p_{\hat{H}|H}(1|1)$ is called the *detection probability* (denoted by $p_{\mathrm{D}}(\phi)$).

In a Neyman-Pearson hypothesis test, the hypothesis testing performance achieved by a strategy ϕ is measured by the miss probability $p_{\mathrm{M}}(\phi)$ if an upper bound constraint on the false-alarm probability $p_{\mathrm{F}}(\phi) \leq \lambda$ is satisfied. The corresponding design objective of the (randomized) hypothesis testing strategy is to minimize the miss probability: Given $0 \leq \lambda \leq 1$,

$$\phi^* = \arg\min_{\phi \in \Phi} p_{\mathrm{M}}(\phi), \text{ s.t. } p_{\mathrm{F}}(\phi) \leq \lambda. \tag{2.7}$$

Note that decreasing $p_{\mathrm{M}}(\phi)$ and decreasing $p_{\mathrm{F}}(\phi)$ are conflicting design objectives. Therefore, an optimal Neyman-Pearson hypothesis testing strategy compromises the two conflicting design objectives.

Given $0 \leq \lambda' \leq 1$, first consider the following optimization problem:

$$\phi^*_{\lambda'} = \arg\min_{\phi \in \Phi} p_{\mathrm{M}}(\phi), \text{ s.t. } p_{\mathrm{F}}(\phi) = \lambda'. \tag{2.8}$$

By introducing a non-negative Lagrange multiplier ρ', a Lagrangian can be formulated as

$$\begin{aligned} L\left(p_{\hat{H}|Y}\right) &= \int_{\mathcal{Y}} p_{\hat{H}|Y}(0|y) f_{Y|H}(y|1) dy + \rho' \left(\int_{\mathcal{Y}} p_{\hat{H}|Y}(1|y) f_{Y|H}(y|0) dy - \lambda' \right) \\ &= \int_{\mathcal{Y}} p_{\hat{H}|Y}(0|y) \left(f_{Y|H}(y|1) - \rho' f_{Y|H}(y|0) \right) dy + \rho' \left(1 - \lambda'\right). \end{aligned} \tag{2.9}$$

The strategy to minimize the Lagrangian is a deterministic LRT as

$$\hat{H} = \begin{cases} 0, \text{ if } \dfrac{f_{Y|H}(y|0)}{f_{Y|H}(y|1)} \geq \dfrac{1}{\rho'} \\ 1, \text{ otherwise} \end{cases}. \tag{2.10}$$

From Assumption 2.1, choose a non-negative ρ' with a corresponding set $\mathcal{A}(\rho')$ such that

$$\int_{\mathcal{A}^c(\rho')} f_{Y|H}\left(y|0\right) dy = \lambda'. \tag{2.11}$$

Then the deterministic LRT in (2.10) under the constraint (2.11) satisfies the false-alarm probability equality constraint in (2.8), i.e., the deterministic LRT (2.10) under the constraint of ρ' in (2.11) is an optimal strategy $\phi^*_{\lambda'}$ for the problem (2.8). Recall Assumption 2.1, there exists a ρ' to satisfy (2.11) for any $0 \leq \lambda' \leq 1$. The optimality of deterministic LRT holds for all $0 \leq \lambda' \leq 1$. Therefore, an optimal strategy of the Neyman-Pearson hypothesis test is a deterministic LRT. From the Neyman-Pearson lemma [12], it is sufficient to consider the following deterministic

LRT for an optimal strategy of the Neyman-Pearson hypothesis test (2.7):

$$\hat{H} = \phi^*(y) = \begin{cases} 0, \text{ if } \dfrac{f_{Y|H}(y|0)}{f_{Y|H}(y|1)} \geq \dfrac{1}{\rho} \\ 1, \text{ otherwise} \end{cases}, \tag{2.12}$$

where the non-negative parameter ρ and the set $\mathcal{A}(\rho)$ satisfy $\int_{\mathcal{A}^c(\rho)} f_{Y|H}(y|0)\, dy = \lambda$. The corresponding false-alarm probability is $p_{\mathrm{F}}(\phi^*) = \lambda$ and the minimal miss probability is $p_{\mathrm{M}}(\phi^*) = \int_{\mathcal{A}(\rho)} f_{Y|H}(y|1)\, dy$.

In a centralized hypothesis testing scenario, the Bayesian and Neyman-Pearson hypothesis tests have been introduced and the optimality of deterministic LRT has been shown. Next, the hypothesis testing operation region is introduced, which provides an alternative way to study hypothesis testing problems.

Operation region

If the decision $\hat{H}$ and the hypothesis H are both binary random variables, a hypothesis testing strategy ϕ can be described by a set of corresponding conditional probabilities: $\left\{p_{\hat{H}|H}(\hat{h}|h)\right\}_{\hat{h},h\in\{0,1\}}$. Due to the property that $\sum_{\hat{h}\in\{0,1\}} p_{\hat{H}|H}(\hat{h}|0) = \sum_{\hat{h}\in\{0,1\}} p_{\hat{H}|H}(\hat{h}|1) = 1$, a pair of conditional probabilities $(p_{\mathrm{F}}(\phi), p_{\mathrm{D}}(\phi))$ can completely characterize the corresponding strategy ϕ. Define the operation point achieved by a strategy ϕ by $\boldsymbol{p}(\phi) \triangleq (p_{\mathrm{F}}(\phi), p_{\mathrm{D}}(\phi))$. Then, the hypothesis testing operation region $\mathcal{R}$ is a set consisting of operation points achieved by all feasible (randomized) hypothesis testing strategies: $\mathcal{R} \triangleq \{\boldsymbol{p}(\phi)\,|\phi \in \Phi\}$. In Figure 2.1, an operation region is illustrated.

If the continuous random observation Y satisfies Assumption 2.1, it has been shown that a deterministic LRT can achieve the minimal miss probability, and equivalently the maximal detection probability, under the constraint that the false-alarm probability is equal to a certain value. That means all operation points on the operation region upper boundary, which is commonly known as the receiver operating characteristic (ROC) curve, can be achieved by deterministic LRTs. It can be shown that all operation points on the operation region lower boundary, which is commonly known as the inverse ROC curve, can also be achieved by deterministic LRTs. This claim can be justified by solving the following optimization problem: Given $0 \leq \lambda'' \leq 1$,

$$\phi^*_{\lambda''} = \arg\max_{\phi\in\Phi} p_{\mathrm{M}}(\phi), \text{ s.t. } p_{\mathrm{F}}(\phi) = \lambda''. \tag{2.13}$$

Following a similar analysis method of the optimization problem (2.8), an optimal strategy of the problem (2.13) is the following deterministic LRT:

$$\hat{H} = \phi^*_{\lambda''}(y) = \begin{cases} 0, \text{ if } \dfrac{f_{Y|H}(y|0)}{f_{Y|H}(y|1)} \leq \dfrac{1}{\rho''} \\ 1, \text{ otherwise} \end{cases}, \tag{2.14}$$

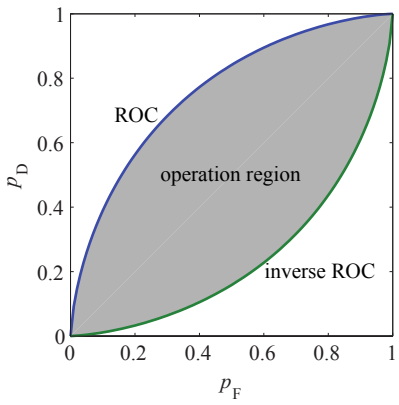


Figure 2.1: A hypothesis testing operation region when the hypothesis H and the decision $\hat{H}$ are both binary random variables; and the continuous random observation Y is generated following $Y|H=0 \sim \mathcal{N}(0,1)$ or $Y|H=1 \sim \mathcal{N}(1,1)$.

where the non-negative parameter ρ'' and the set $\mathcal{A}(\rho'')$ satisfy $\int_{\mathcal{A}(\rho'')} f_{Y|H}(y|0)\,dy = \lambda''$. Note that the deterministic LRTs achieving operation points on the upper and lower boundaries are different in the inequality direction of the threshold test.

Property 2.1. *Given a binary hypothesis H, a binary decision $\hat{H}$, and a continuous random observation Y satisfying Assumption 2.1, the following properties of the operation region $\mathcal{R}$ can be implied from the ROC properties summarized in [59]:*

1. *The operation region $\mathcal{R}$ is a convex set and is point symmetric with respect to the operation point $(0.5, 0.5)$;*
2. *The ROC curve (upper boundary) is concave, non-decreasing, with two end operation points $(0,0)$, $(1,1)$, and above the line $p_{\mathrm{D}} = p_{\mathrm{F}}$;*
3. *The inverse ROC curve (lower boundary) is convex, non-decreasing, with two end operation points $(0,0)$, $(1,1)$, and below the line $p_{\mathrm{D}} = p_{\mathrm{F}}$;*
4. *All operation points on the ROC and inverse ROC curves can be achieved by deterministic LRTs;*
5. *All inner operation points can be achieved by randomized strategies of deterministic LRTs.*

In the context of the introduced centralized hypothesis testing scenario, the optimality of deterministic LRT in the Bayesian and Neyman-Pearson hypothesis tests can be justified through the operation region as well.

For the Neyman-Pearson hypothesis test (2.7), the minimal miss probability, or equivalently the maximal detection probability, subject to an upper bound constraint on the false-alarm probability corresponds to an intersection point of the ROC curve and the line $p_{\mathrm{F}} = \lambda$. The deterministic LRT which achieves the intersection point is an optimal Neyman-Pearson hypothesis testing strategy.

For the Bayesian hypothesis test (2.2), the optimization objective, the Bayesian risk, can be rewritten as an affine function of $p_{\mathrm{F}}(\phi)$ and $p_{\mathrm{D}}(\phi)$ as

$$\begin{aligned} r(\phi) &= \mathrm{E}\left[c(\hat{H}, H)\right] = \sum_{\hat{h},h\in\{0,1\}} p_{\hat{H}|H}(\hat{h}|h)p_H(h)c(\hat{h},h) \\ &= p_H(0)(c(1,0)-c(0,0))p_{\mathrm{F}}(\phi) + p_H(1)(c(1,1)-c(0,1))p_{\mathrm{D}}(\phi) \\ &\quad + p_H(0)c(0,0) + p_H(1)c(0,1). \end{aligned} \tag{2.15}$$

To minimize the affine objective over the convex operation region, the minimization is achieved at a boundary point which has a supporting hyperplane in parallel with the affine objective hyperplane. The deterministic LRT which achieves the boundary point is an optimal Bayesian hypothesis testing strategy.

Discrete random observation

Until now, the optimality of deterministic LRT is justified in the context of the introduced centralized hypothesis testing scenario where the continuous random observation satisfies Assumption 2.1. However, the optimality of deterministic LRT needs to be revised if the observation is a discrete random variable.

Suppose that the discrete random observation Y is generated following a likelihood p.m.f. $p_{Y|H}(\cdot|0)$ or $p_{Y|H}(\cdot|1)$. Given a hypothesis testing strategy ϕ, the Bayesian risk is

$$r(\phi) = \mathrm{E}\left[c(\hat{H}, H)\right] = \sum_{y\in\mathcal{Y}} \sum_{\hat{h},h\in\{0,1\}} p_{\hat{H}|Y}(\hat{h}|y)p_{Y|H}(y|h)p_H(h)c(\hat{h},h), \tag{2.16}$$

where the conditional p.m.f. $p_{\hat{H}|Y}$ corresponds to the strategy ϕ. An optimal strategy of the Bayesian hypothesis test (2.2) is the following deterministic likelihood-based test

$$\hat{H} = \phi^*(y) = \arg\min_{\hat{h}\in\{0,1\}} \sum_{h\in\{0,1\}} p_{Y|H}(y|h)p_H(h)c(\hat{h},h), \tag{2.17}$$

which can be rewritten as an equivalent deterministic LRT. Therefore, the optimality of deterministic LRT holds for the Bayesian hypothesis test when the observation is a discrete random variable.

Given a strategy ϕ and the conditional p.m.f. $p_{\hat{H}|Y}$, the corresponding conditional probability $p_{\hat{H}|H}(\hat{h}|h)$, with $\hat{h}$, $h \in \{0,1\}$, is given in terms of $p_{\hat{H}|Y}$ as

$$p_{\hat{H}|H}(\hat{h}|h) = \sum_{y\in\mathcal{Y}} p_{\hat{H}|Y}(\hat{h}|y)p_{Y|H}(y|h). \tag{2.18}$$

Given a non-negative parameter ρ, define a set $\mathcal{A}(\rho) = \left\{ y \left| \frac{p_{Y|H}(y|0)}{p_{Y|H}(y|1)} \geq \frac{1}{\rho} \right. \right\}$. If a non-negative parameter ρ' and the set $\mathcal{A}(\rho')$ satisfy $\sum_{y \in \mathcal{A}^c(\rho')} p_{Y|H}(y|0) = \lambda'$, it follows from the method of Lagrange multiplier that an optimal strategy of the problem (2.8) is a deterministic LRT as

$$\hat{H} = \phi^*_{\lambda'}(y) = \begin{cases} 0, & \text{if } \dfrac{p_{Y|H}(y|0)}{p_{Y|H}(y|1)} \geq \dfrac{1}{\rho'} \\ 1, & \text{otherwise} \end{cases}. \tag{2.19}$$

However, the range of the function $\sum_{y \in \mathcal{A}^c(\rho)} p_{Y|H}(y|0)$ is discrete, i.e., it is not always possible to find a value of ρ to obtain a desired value of $\sum_{y \in \mathcal{A}^c(\rho)} p_{Y|H}(y|0)$. Then, the method of Lagrange multiplier cannot be used. Instead, the discussion on the optimality of deterministic LRT in a Neyman-Pearson hypothesis test with a discrete random observation can be more easily explained using the hypothesis testing operation region.

When the observation is a discrete random variable, the operation region $\mathcal{R}$ is a convex set since randomized strategies are allowed; there are a finite number of operation points achieved by deterministic hypothesis testing strategies; and all the other operation points can be achieved by randomized strategies. Since the Bayesian risk can be expressed as an affine function of $\boldsymbol{p}(\phi) \triangleq (p_{\mathrm{F}}(\phi), p_{\mathrm{D}}(\phi))$ as (2.15), an optimal strategy of the Bayesian hypothesis test achieves an operation point on the operation region boundary. From the optimality of deterministic LRT in the Bayesian hypothesis test, it follows that all boundary operation points achieved by deterministic strategies can be achieved by deterministic LRTs. Therefore, the characteristics of the operation region and the boundary can be obtained by studying the deterministic LRTs. When the observation is a discrete random variable, properties of the operation region are summarized in Property 2.2 and an illustration of operation region is shown in Figure 2.2.

Property 2.2. *Given a binary hypothesis H, a binary decision $\hat{H}$, and a discrete random observation Y, the hypothesis testing operation region $\mathcal{R}$ has the following properties:*

1. *The operation region $\mathcal{R}$ is a convex set and is point symmetric with respect to the operation point $(0.5, 0.5)$;*
2. *The ROC curve (upper boundary) is concave, non-decreasing, with two end operation points $(0,0)$, $(1,1)$, and above the line $p_{\mathrm{D}} = p_{\mathrm{F}}$;*
3. *The inverse ROC curve (lower boundary) is convex, non-decreasing, with two end operation points $(0,0)$, $(1,1)$, and below the line $p_{\mathrm{D}} = p_{\mathrm{F}}$;*
4. *On the ROC and inverse ROC curves, all "corner" points can be achieved by deterministic LRTs and the other operation points can be achieved by randomized strategies of two deterministic LRTs;*

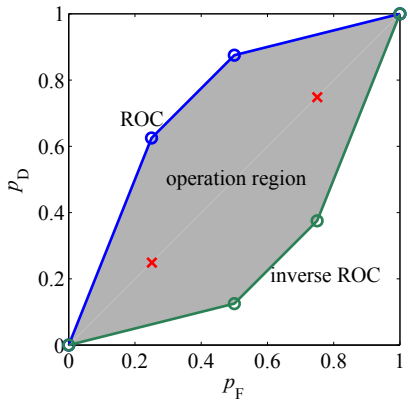


Figure 2.2: A hypothesis testing operation region when the hypothesis H and the decision $\hat{H}$ are both binary random variables; and the discrete random observation Y is generated following $p_{Y|H}(0|0) = \frac{1}{2}$, $p_{Y|H}(1|0) = \frac{1}{4}$, $p_{Y|H}(2|0) = \frac{1}{4}$, or $p_{Y|H}(0|1) = \frac{1}{8}$, $p_{Y|H}(1|1) = \frac{5}{8}$, $p_{Y|H}(2|1) = \frac{1}{4}$. On the ROC and inverse ROC curves, the circle operation points can be achieved by deterministic LRTs and the other operation points can be achieved by randomized strategies of deterministic LRTs. The red cross operation points can be achieved by non-LRT deterministic strategies.

5. *All inner operation points can be achieved by randomized strategies of deterministic LRTs.*

Based on Property 2.2, an optimal strategy in the Neyman-Pearson hypothesis test with a discrete random observation can be a deterministic LRT or a randomized strategy of two deterministic LRTs. Therefore, the optimality of deterministic LRT does not always hold when the observation in the Neyman-Pearson hypothesis test is a discrete random variable.

2.2 Asymptotic Hypothesis Testing Performances

In the previous discussion, the observation is modeled by a random variable Y. The obtained results can easily be extended to a general case of having a sequence of observations modeled by a random vector Y^n through substituting Y with Y^n. Obviously, the optimal hypothesis testing performance does not degrade with more observations. It is therefore interesting to characterize the improvement rate of the hypothesis testing performance with respect to the increasing length of the random observation sequence.

Consider a centralized hypothesis testing scenario where the hypothesis H is a binary random variable with prior probabilities $p_H(0)$ and $p_H(1)$; each discrete

random observation Y_i in the observation sequence Y^n is identically independently distributed (i.i.d.) and following the p.m.f. $p_{Y|H}(\cdot|0)$ or $p_{Y|H}(\cdot|1)$; and the binary decision $\hat{H}$ is made based on the random observation sequence Y^n and following a deterministic hypothesis testing strategy $\phi^n : \mathcal{Y}^n \to \{0,1\}$ to infer the correct hypothesis. Given a deterministic strategy ϕ^n, let $\mathcal{A}_n$ and $\mathcal{A}_n^c$ denote the decision regions for hypothesis 0 and hypothesis 1, respectively, i.e.,

$$\hat{H} = \phi^n(y^n) = \begin{cases} 0, \text{ if } y^n \in \mathcal{A}_n \\ 1, \text{ if } y^n \in \mathcal{A}_n^c \end{cases}.$$

In the Bayesian hypothesis test, the decision costs are assigned as $c(0,0) = c(1,1) = 0$ and $c(0,1) = c(1,0) = 1$, i.e., the decision cost is 0 if a correct decision is made or 1 if a wrong decision is made. With the decision cost assignment and given a deterministic hypothesis testing strategy ϕ^n, the corresponding Bayesian risk reduces to the hypothesis testing error probability:

$$\begin{aligned} p_{\mathrm{e}}(\phi^n) &= p_{\hat{H},H}(1,0) + p_{\hat{H},H}(0,1) \\ &= \sum_{y^n \in \mathcal{A}_n^c} p_{Y^n|H}(y^n|0) p_H(0) + \sum_{y^n \in \mathcal{A}_n} p_{Y^n|H}(y^n|1) p_H(1). \end{aligned} \tag{2.20}$$

An optimal deterministic Bayesian hypothesis testing strategy ϕ^{n*} achieves the minimal error probability $p_{\mathrm{e}}(\phi^{n*})$. As the observation sequence length n increases, the minimal error probability $p_{\mathrm{e}}(\phi^{n*})$ decreases. In the Bayesian hypothesis test, the hypothesis testing performance improvement rate can be characterized by the exponential decay rate of the minimal error probability $\frac{1}{n} \log \frac{1}{p_{\mathrm{e}}(\phi^{n*})}$. In the following theorem [11], it is shown that the asymptotic exponential decay rate of the minimal error probability can be specified by a Chernoff information.

Theorem 2.1.

$$\begin{aligned} \lim_{n\to\infty} \frac{1}{n} \log \frac{1}{p_{\mathrm{e}}(\phi^{n*})} &= \mathrm{C}(p_{Y|H}(\cdot|0), p_{Y|H}(\cdot|1)) \\ &= \max_{0 \le \tau \le 1} \left\{ -\log \left(\sum_{y \in \mathcal{Y}} p_{Y|H}^{\tau}(y|0) p_{Y|H}^{1-\tau}(y|1) \right) \right\}. \end{aligned} \tag{2.21}$$

Remark 2.4. *Note that the asymptotic exponential decay rate of the minimal error probability does not depend on the hypothesis prior distribution.*

In the Neyman-Pearson hypothesis test, an optimal deterministic hypothesis testing strategy ϕ^{n*} satisfies an upper bound constraint on the false-alarm probability $p_{\mathrm{F}}(\phi^{n*}) \le \lambda$ and achieves the minimal miss probability $p_{\mathrm{M}}(\phi^{n*})$. The hypothesis testing performance improvement rate can be characterized by the exponential decay rate of the minimal miss probability $\frac{1}{n} \log \frac{1}{p_{\mathrm{M}}(\phi^{n*})}$. In the following Stein's

lemma [12], it is shown that the asymptotic exponential decay rate of the minimal miss probability can be specified by a Kullback-Leibler divergence.

Theorem 2.2 (Stein's lemma)**.** *For all* $\lambda \in (0,1)$*,*

$$\lim_{n\to\infty} \frac{1}{n} \log \frac{1}{p_{\mathrm{M}}(\phi^{n*})} = \mathrm{D}(p_{Y|H}(\cdot|0)||p_{Y|H}(\cdot|1)) = \sum_{y\in\mathcal{Y}} p_{Y|H}(y|0) \log \frac{p_{Y|H}(y|0)}{p_{Y|H}(y|1)}. \tag{2.22}$$

Remark 2.5. *Consider that the observation sequence* Y^n *consists of i.i.d. continuous random observations which are generated following the p.d.f.* $f_{Y|H}(\cdot|0)$ *or* $f_{Y|H}(\cdot|1)$*. Theorems 2.1-2.2 hold and the asymptotic exponential decay rates are specified by the Chernoff information* $\mathrm{C}(f_{Y|H}(\cdot|0), f_{Y|H}(\cdot|1))$ *as shown in [48] and the Kullback-Leibler divergence* $\mathrm{D}(f_{Y|H}(\cdot|0)||f_{Y|H}(\cdot|1))$ *as shown in [10].*

2.3 Distributed Hypothesis Testing Problems

In practice, a hypothesis test can be done by a network instead of a single decision node. Depending on the processing capability, energy efficiency, topology, application, and etc., there are different distributed hypothesis testing settings. In this section, the Bayesian and Neyman-Pearson hypothesis tests are revisited in a parallel distributed hypothesis testing network.

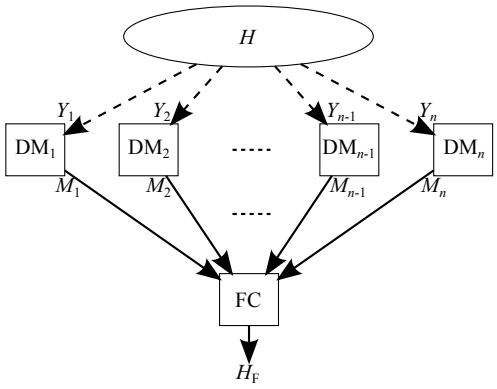


Figure 2.3: A parallel distributed hypothesis testing network.

The parallel distributed hypothesis testing network in Figure 2.3 is described as follows: There is a binary hypothesis H which can take the value 0 or 1; a continuous random observation Y_i of the remote decision maker DM_i, $1 \le i \le n$, is independently generated conditioned on hypothesis 0 following a p.d.f. $f_{Y_i|H}(\cdot|0)$ or on hypothesis 1 following a p.d.f. $f_{Y_i|H}(\cdot|1)$, and satisfies Assumption 2.1; for

all $1 \leq i \leq n$, DM_i independently makes a binary remote decision M_i based on the observation Y_i and following a (randomized) remote strategy $\phi_i : \mathcal{Y}_i \to \{0,1\}$; and a binary fusion decision H_F is made at the fusion center (FC) based on the received remote decisions M^n and following a (randomized) fusion strategy $\phi_\mathrm{F} : \{0,1\}^n \to \{0,1\}$ to infer the correct hypothesis.

Distributed Bayesian hypothesis test

Given a fusion decision cost assignment $\{c_\mathrm{F}(h_\mathrm{F}, h)\}_{h_\mathrm{F}, h \in \{0,1\}}$, the Bayesian risk of a distributed hypothesis testing network design $(\phi_1, \ldots, \phi_n, \phi_\mathrm{F})$ is the expected fusion decision cost:

$$\begin{aligned} r_\mathrm{F}(\phi_1, \ldots, \phi_n, \phi_\mathrm{F}) &= \mathrm{E}\left[c_\mathrm{F}(H_\mathrm{F}, H)\right] \\ &= \int_{\mathcal{Y}^n} \sum_{m^n \in \{0,1\}^n, h_\mathrm{F}, h \in \{0,1\}} p_{H_\mathrm{F}|M^n}(h_\mathrm{F}|m^n) \\ &\qquad \prod_{i=1}^{n} p_{M_i|Y_i}(m_i|y_i) f_{Y_i|H}(y_i|h) p_H(h) c_\mathrm{F}(h_\mathrm{F}, h) dy^n, \end{aligned} \tag{2.23}$$

where the conditional p.m.f.s $p_{H_\mathrm{F}|M^n}$ and $p_{M_i|Y_i}$ correspond to the fusion strategy ϕ_F and the remote strategy ϕ_i, respectively. In the Bayesian hypothesis test, the optimal distributed hypothesis testing network is designed to minimize the Bayesian risk:

$$(\phi_1^*, \ldots, \phi_n^*, \phi_\mathrm{F}^*) = \underset{(\phi_1, \ldots, \phi_n, \phi_\mathrm{F}) \in \Phi_1 \times \cdots \times \Phi_n \times \Phi_\mathrm{F}}{\arg\min} r_\mathrm{F}(\phi_1, \ldots, \phi_n, \phi_\mathrm{F}). \tag{2.24}$$

The optimality of deterministic LRT holds for the distributed Bayesian hypothesis test (2.24). This claim can be verified based on the person-by-person optimality argument which is made concrete in the following lemma.

Lemma 2.1 (Person-by-person optimality)**.** *Given an optimal distributed Bayesian hypothesis testing network design $(\phi_1^*, \ldots, \phi_n^*, \phi_\mathrm{F}^*)$, an optimal strategy has to be person-by-person optimal when the other optimal strategies are fixed, i.e.,*

$$\begin{aligned} \phi_1^* &= \underset{\phi_1 \in \Phi_1}{\arg\min}\, r_\mathrm{F}(\phi_1, \phi_2^*, \ldots, \phi_n^*, \phi_\mathrm{F}^*); \\ \phi_n^* &= \underset{\phi_n \in \Phi_n}{\arg\min}\, r_\mathrm{F}(\phi_1^*, \ldots, \phi_{n-1}^*, \phi_n, \phi_\mathrm{F}^*); \\ \phi_i^* &= \underset{\phi_i \in \Phi_i}{\arg\min}\, r_\mathrm{F}(\phi_1^*, \ldots, \phi_i, \ldots, \phi_n^*, \phi_\mathrm{F}^*),\ \forall 2 \leq i \leq n-1; \\ \phi_\mathrm{F}^* &= \underset{\phi_\mathrm{F} \in \Phi_\mathrm{F}}{\arg\min}\, r_\mathrm{F}(\phi_1^*, \ldots, \phi_n^*, \phi_\mathrm{F}). \end{aligned} \tag{2.25}$$

Proof. Given $2 \leq i \leq n-1$ and fixing the optimal strategies other than ϕ_i, assume that ϕ_i^* is not an optimizer of the optimization of ϕ_i in (2.25). That means there

exists a remote strategy $\phi_i^{\#} \in \Phi_i$ leading to a better distributed hypothesis testing design, i.e.,

$$r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_i^{\#}, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*) < r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_i^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*).$$

It contradicts with that $(\phi_1^*, \ldots, \phi_i^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)$ is an optimal distributed hypothesis testing network design which achieves the minimal Bayesian risk. Therefore, the assumption does not hold.

Following from the same analysis, the other equalities in (2.25) can also be verified. □

From the person-by-person optimality argument, an optimal strategy of the distributed Bayesian hypothesis test (2.24) can be characterized by studying the corresponding person-by-person optimization in (2.25).

Given $2 \leq i \leq n-1$, the Bayesian risk of the person-by-person optimization of remote strategy ϕ_i reduces to

$$\begin{aligned}
&r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_i, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*) \\
&= \int_{\mathcal{Y}_i} \sum_{m_i \in \{0,1\}} p_{M_i|Y_i}(m_i|y_i) \int_{\mathcal{Y}^{n\setminus i}} \sum_{m^{n\setminus i} \in \{0,1\}^{n-1}, h_{\mathrm{F}}, h \in \{0,1\}} p^*_{H_{\mathrm{F}}|M^n}(h_{\mathrm{F}}|m^{n\setminus i}, m_i) \\
&\qquad f_{Y_i|H}(y_i|h) \prod_{k=1, k\neq i}^{n} p^*_{M_k|Y_k}(m_k|y_k) f_{Y_k|H}(y_k|h) p_H(h) c_{\mathrm{F}}(h_{\mathrm{F}}, h) dy^{n\setminus i} dy_i,
\end{aligned} \tag{2.26}$$

where the conditional p.m.f.s $p^*_{H_{\mathrm{F}}|M^n}$, $p^*_{M_k|Y_k}$, and $p_{M_i|Y_i}$ correspond to the optimal fusion strategy ϕ_{F}^*, the optimal remote strategy ϕ_k^*, and the remote strategy ϕ_i, respectively. To minimize the Bayesian risk, an optimal remote strategy of the person-by-person optimization problem is the following deterministic likelihood-based test:

$$\begin{aligned}
M_i = \phi_i^*(y_i) = \ &\arg\min_{m_i \in \{0,1\}} \int_{\mathcal{Y}^{n\setminus i}} \sum_{m^{n\setminus i} \in \{0,1\}^{n-1}, h_{\mathrm{F}}, h \in \{0,1\}} p^*_{H_{\mathrm{F}}|M^n}(h_{\mathrm{F}}|m^{n\setminus i}, m_i) \\
&f_{Y_i|H}(y_i|h) \prod_{k=1, k\neq i}^{n} p^*_{M_k|Y_k}(m_k|y_k) f_{Y_k|H}(y_k|h) p_H(h) c_{\mathrm{F}}(h_{\mathrm{F}}, h) dy^{n\setminus i}.
\end{aligned} \tag{2.27}$$

Define

$$\begin{aligned}
c_i^*(m_i, h) \triangleq \int_{\mathcal{Y}^{n\setminus i}} &\sum_{m^{n\setminus i} \in \{0,1\}^{n-1}, h_{\mathrm{F}} \in \{0,1\}} p^*_{H_{\mathrm{F}}|M^n}(h_{\mathrm{F}}|m^{n\setminus i}, m_i) \\
&\prod_{k=1, k\neq i}^{n} p^*_{M_k|Y_k}(m_k|y_k) f_{Y_k|H}(y_k|h) c_{\mathrm{F}}(h_{\mathrm{F}}, h) dy^{n\setminus i}.
\end{aligned} \tag{2.28}$$

Depending on the sign of $c_i^*(1,0) - c_i^*(0,0)$, the optimal deterministic likelihood-based remote test (2.27) reduces to a deterministic LRT:

$$M_i = \phi_i^*(y_i) = \begin{cases} 0, & \text{if } \dfrac{f_{Y_i|H}(y_i|0)}{f_{Y_i|H}(y_i|1)} \geq \dfrac{p_H(1)(c_i^*(0,1) - c_i^*(1,1))}{p_H(0)(c_i^*(1,0) - c_i^*(0,0))} \\ 1, & \text{otherwise} \end{cases}, \tag{2.29}$$

or

$$M_i = \phi_i^*(y_i) = \begin{cases} 0, & \text{if } \dfrac{f_{Y_i|H}(y_i|0)}{f_{Y_i|H}(y_i|1)} \leq \dfrac{p_H(1)(c_i^*(0,1) - c_i^*(1,1))}{p_H(0)(c_i^*(1,0) - c_i^*(0,0))} \\ 1, & \text{otherwise} \end{cases}. \tag{2.30}$$

The study on the person-by-person optimization of the remote strategy ϕ_1 (resp. ϕ_n) similarly leads to that an optimal remote strategy ϕ_1^* (resp. ϕ_n^*) is a deterministic LRT.

When all the optimal remote decision strategies are fixed, the person-by-person optimization of the fusion strategy ϕ_{F} is a centralized hypothesis testing problem with a discrete random observation sequence M^n. The corresponding fusion observation likelihoods $p^*_{M^n|H}(\cdot|0)$ and $p^*_{M^n|H}(\cdot|1)$ are in terms of the remote observation likelihoods and the optimal remote strategies as

$$p^*_{M^n|H}(m^n|h) = \int_{\mathcal{Y}^n} \prod_{i=1}^{n} p^*_{M_i|Y_i}(m_i|y_i) f_{Y_i|H}(y_i|h) dy^n. \tag{2.31}$$

The Bayesian risk of the person-by-person optimization of ϕ_{F} is

$$\begin{aligned} & r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}) \\ = & \sum_{m^n \in \{0,1\}^n} \sum_{h_{\mathrm{F}} \in \{0,1\}} p_{H_{\mathrm{F}}|M^n}(h_{\mathrm{F}}|m^n) \sum_{h \in \{0,1\}} p^*_{M^n|H}(m^n|h) p_H(h) c_{\mathrm{F}}(h_{\mathrm{F}}, h). \end{aligned} \tag{2.32}$$

An optimal fusion strategy to minimize the Bayesian risk (2.32) is the following deterministic likelihood-based test:

$$H_{\mathrm{F}} = \phi_{\mathrm{F}}^*(m^n) = \arg\min_{h_{\mathrm{F}} \in \{0,1\}} \sum_{h \in \{0,1\}} p^*_{M^n|H}(m^n|h) p_H(h) c_{\mathrm{F}}(h_{\mathrm{F}}, h). \tag{2.33}$$

Depending on the sign of $c_{\mathrm{F}}(1,0) - c_{\mathrm{F}}(0,0)$, the optimal deterministic fusion strategy (2.33) reduces to a deterministic LRT:

$$H_{\mathrm{F}} = \phi_{\mathrm{F}}^*(m^n) = \begin{cases} 0, & \text{if } \dfrac{p^*_{M^n|H}(m^n|0)}{p^*_{M^n|H}(m^n|1)} \geq \dfrac{p_H(1)(c_{\mathrm{F}}(0,1) - c_{\mathrm{F}}(1,1))}{p_H(0)(c_{\mathrm{F}}(1,0) - c_{\mathrm{F}}(0,0))} \\ 1, & \text{otherwise} \end{cases}, \tag{2.34}$$

or

$$H_{\mathrm{F}} = \phi_{\mathrm{F}}^*(m^n) = \begin{cases} 0, \text{ if } \dfrac{p^*_{M^n|H}(m^n|0)}{p^*_{M^n|H}(m^n|1)} \leq \dfrac{p_H(1)(c_{\mathrm{F}}(0,1) - c_{\mathrm{F}}(1,1))}{p_H(0)(c_{\mathrm{F}}(1,0) - c_{\mathrm{F}}(0,0))} \\ 1, \text{ otherwise} \end{cases}. \tag{2.35}$$

Therefore, it is sufficient to consider deterministic LRTs for decision strategies in an optimal distributed Bayesian hypothesis testing network design.

Remark 2.6. *If remote observations in Y^n are discrete random variables, the optimality of deterministic LRT still holds for an optimal distributed Bayesian hypothesis testing network design.*

Remark 2.7. *If the hypothesis and decisions are not binary, it is sufficient to consider deterministic likelihood-based tests in the form of (2.27) or (2.33) for decision strategies in an optimal distributed Bayesian hypothesis testing network design.*

Distributed Neyman-Pearson hypothesis test

Given a distributed hypothesis testing network design $(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}})$, the miss probability and false-alarm probability of fusion decision are

$$\begin{aligned} p_{\mathrm{FM}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) &= p_{H_{\mathrm{F}}|H}(0|1) \\ &= \int_{\mathcal{Y}^n} \sum_{m^n \in \{0,1\}^n} p_{H_{\mathrm{F}}|M^n}(0|m^n) \prod_{i=1}^n p_{M_i|Y_i}(m_i|y_i) f_{Y_i|H}(y_i|1) dy^n, \\ p_{\mathrm{FF}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) &= p_{H_{\mathrm{F}}|H}(1|0) \\ &= \int_{\mathcal{Y}^n} \sum_{m^n \in \{0,1\}^n} p_{H_{\mathrm{F}}|M^n}(1|m^n) \prod_{i=1}^n p_{M_i|Y_i}(m_i|y_i) f_{Y_i|H}(y_i|0) dy^n, \end{aligned} \tag{2.36}$$

where the conditional p.m.f.s $p_{H_{\mathrm{F}}|M^n}$ and $p_{M_i|Y_i}$ correspond to the fusion strategy ϕ_{F} and the remote strategy ϕ_i, respectively. In the Neyman-Pearson hypothesis test, an optimal distributed hypothesis testing network is designed to minimize the miss probability of fusion decision subject to an upper bound $0 \leq \lambda \leq 1$ on the false-alarm probability of fusion decision:

$$\begin{aligned} (\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*) = \underset{(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) \in \Phi_1 \times \cdots \times \Phi_n \times \Phi_{\mathrm{F}}}{\arg\min} & \quad p_{\mathrm{FM}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) \\ \text{s.t.} & \quad p_{\mathrm{FF}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) \leq \lambda. \end{aligned} \tag{2.37}$$

Give an optimal distributed hypothesis testing network design $(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)$ for the Neyman-Pearson hypothesis test. From the person-by-person optimality argument, it follows that

$$\phi_{\mathrm{F}}^* = \underset{\phi_{\mathrm{F}} \in \Phi_{\mathrm{F}}}{\arg\min}\, p_{\mathrm{FM}}(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}), \text{ s.t. } p_{\mathrm{FF}}(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}) \leq \lambda. \tag{2.38}$$

In the centralized hypothesis testing scenario with a discrete random observation, the optimality of deterministic LRT does not always hold for the Neyman-Pearson hypothesis test. Note that the FC has a binary random observation sequence in the distributed hypothesis testing network. Therefore, an optimal fusion strategy for the distributed Neyman-Pearson hypothesis test can be a deterministic LRT or a randomized strategy of two deterministic LRTs. Further, the false-alarm probability of fusion decision achieved by an optimal distributed Neyman-Pearson hypothesis testing network is equal to λ according to Property 2.2.

Based on the analysis on the person-by-person optimization of the fusion strategy, the Neyman-Pearson hypothesis test (2.37) can be slightly modified as

$$\begin{aligned}(\phi_1^*,\ldots,\phi_n^*,\phi_{\rm F}^*) = \mathop{\arg\min}_{(\phi_1,\ldots,\phi_n,\phi_{\rm F})\in\Phi_1\times\cdots\times\Phi_n\times\Phi_{\rm F}} & \quad p_{\rm FM}(\phi_1,\ldots,\phi_n,\phi_{\rm F}) \\ \text{s.t.} & \quad p_{\rm FF}(\phi_1,\ldots,\phi_n,\phi_{\rm F}) = \lambda.\end{aligned} \tag{2.39}$$

From the person-by-person optimality argument, it follows for all $2 \le i \le n-1$ that

$$\phi_i^* = \mathop{\arg\min}_{\phi_i\in\Phi_i} p_{\rm FM}(\phi_1^*,\ldots,\phi_i,\ldots,\phi_n^*,\phi_{\rm F}^*),\ \text{s.t.}\ p_{\rm FF}(\phi_1^*,\ldots,\phi_i,\ldots,\phi_n^*,\phi_{\rm F}^*) = \lambda. \tag{2.40}$$

Define

$$\begin{aligned}a_i^*(m_i,h_{\rm F},h) \triangleq \int_{\mathcal{Y}^{n\setminus i}} & \sum_{m^{n\setminus i}\in\{0,1\}^{n-1}} p^*_{H_{\rm F}|M^n}(h_{\rm F}|m^{n\setminus i},m_i) \\ & \prod_{k=1,k\neq i}^{n} p^*_{M_k|Y_k}(m_k|y_k) f_{Y_k|H}(y_k|h)dy^{n\setminus i}.\end{aligned} \tag{2.41}$$

Then, the miss probability and false-alarm probability of fusion decision can be rewritten as

$$\begin{aligned}p_{\rm FM}(\phi_1^*,\ldots,\phi_i,\ldots,\phi_n^*,\phi_{\rm F}^*) &= \sum_{m_i\in\{0,1\}} a_i^*(m_i,0,1)\int_{\mathcal{Y}_i} p_{M_i|Y_i}(m_i|y_i)f_{Y_i|H}(y_i|1)dy_i \\ &= a_i^*(0,0,1)p_{M_i|H}(0|1) + a_i^*(1,0,1)p_{M_i|H}(1|1) \\ &= a_i^*(0,0,1) + (a_i^*(1,0,1) - a_i^*(0,0,1))p_{i\rm D}(\phi_i), \\ p_{\rm FF}(\phi_1^*,\ldots,\phi_i,\ldots,\phi_n^*,\phi_{\rm F}^*) &= \sum_{m_i\in\{0,1\}} a_i^*(m_i,1,0)\int_{\mathcal{Y}_i} p_{M_i|Y_i}(m_i|y_i)f_{Y_i|H}(y_i|0)dy_i \\ &= a_i^*(0,1,0)p_{M_i|H}(0|0) + a_i^*(1,1,0)p_{M_i|H}(1|0) \\ &= a_i^*(0,1,0) + (a_i^*(1,1,0) - a_i^*(0,1,0))p_{i\rm F}(\phi_i),\end{aligned} \tag{2.42}$$

where $p_{i\rm D}$ and $p_{i\rm F}$ denote the detection probability and false-alarm probability of remote decision of DM_i, respectively. Thus, the person-by-person optimization

problem (2.40) reduces to

$$\begin{aligned}\phi_i^* = \arg\min_{\phi_i \in \Phi_i} \; & a_i^*(0,0,1) + (a_i^*(1,0,1) - a_i^*(0,0,1))p_{i\mathrm{D}}(\phi_i) \\ \text{s.t.} \quad & a_i^*(0,1,0) + (a_i^*(1,1,0) - a_i^*(0,1,0))p_{i\mathrm{F}}(\phi_i) = \lambda.\end{aligned}$$

Based on Property 2.1, an optimal remote strategy ϕ_i^*, $2 \le i \le n-1$, is a deterministic LRT:

$$\text{If } a_i^*(1,0,1) - a_i^*(0,0,1) \le 0,\ M_i = \phi_i^*(y_i) = \begin{cases} 0, & \text{if } \dfrac{f_{Y_i|H}(y_i|0)}{f_{Y_i|H}(y_i|1)} \ge \dfrac{1}{\rho_i} \\ 1, & \text{otherwise} \end{cases}, \quad (2.43)$$

where non-negative ρ_i and the corresponding set $\mathcal{A}_i(\rho_i) = \left\{ y_i \left| \frac{f_{Y_i|H}(y_i|0)}{f_{Y_i|H}(y_i|1)} \ge \frac{1}{\rho_i} \right. \right\}$ satisfy

$$\int_{\mathcal{A}_i^c(\rho_i)} f_{Y_i|H}(y_i|0)\, dy_i = \frac{\lambda - a_i^*(0,1,0)}{a_i^*(1,1,0) - a_i^*(0,1,0)};$$

or

$$\text{If } a_i^*(1,0,1) - a_i^*(0,0,1) > 0,\ M_i = \phi_i^*(y_i) = \begin{cases} 0, & \text{if } \dfrac{f_{Y_i|H}(y_i|0)}{f_{Y_i|H}(y_i|1)} \le \dfrac{1}{\rho_i} \\ 1, & \text{otherwise} \end{cases}, \quad (2.44)$$

where non-negative ρ_i and the corresponding set $\mathcal{A}_i(\rho_i)$ satisfy

$$\int_{\mathcal{A}_i(\rho_i)} f_{Y_i|H}(y_i|0)\, dy_i = \frac{\lambda - a_i^*(0,1,0)}{a_i^*(1,1,0) - a_i^*(0,1,0)}.$$

The study on the person-by-person optimization of the remote strategy ϕ_1 (resp. ϕ_n) leads to that an optimal remote strategy ϕ_1^* (resp. ϕ_n^*) is a deterministic LRT.

Therefore, it is sufficient to consider deterministic LRTs for remote strategies in an optimal distributed Neyman-Pearson hypothesis testing network design.

Remark 2.8. *If a remote observation Y_i is a discrete random variable, ϕ_i^* in an optimal distributed Neyman-Pearson hypothesis testing network design can be a deterministic LRT or a randomized strategy of two deterministic LRTs.*

Person-by-person optimization algorithm

Using the tool of the person-by-person optimality argument, necessary conditions satisfied by an optimal distributed hypothesis testing network design are characterized for the Bayesian hypothesis test and the Neyman-Pearson hypothesis test. These characteristics are helpful to simplify the algorithm to design an optimal distributed hypothesis testing network.

Person-by-person optimization (PBPO) algorithm [20] is a useful tool for the design of an optimal distributed hypothesis testing network. Fixing other strategies, optimizing the remaining strategy leads to a better or an equivalent distributed hypothesis testing network design. Iteratively running PBPO of all strategies until the hypothesis testing performance does not further improve leads to a locally optimal distributed hypothesis testing network design. Due to the optimality of deterministic LRT, the PBPO of a remote strategy or the fusion strategy in the Bayesian hypothesis test can be constrained to the set of deterministic LRTs without loss of optimality. For the Neyman-Pearson hypothesis test, the PBPO of a remote strategy can also be constrained to the set of deterministic LRTs while the PBPO of the fusion strategy can be constrained to the deterministic LRT or the randomized strategy of two LRTs which achieves the upper bound on the false-alarm probability of fusion decision.

Note that the PBPO algorithm outputs a locally optimal distributed hypothesis testing network design depending on the initial distributed hypothesis testing network design. To "approach" an optimal distributed hypothesis testing network design, the PBPO algorithm needs to be run with a large number of initial distributed hypothesis testing network designs.

2.4 Summary

In this chapter, the fundamentals of hypothesis testing problems are recapitulated. The optimality of deterministic likelihood-based test (or LRT) is investigated in different hypothesis testing problems. To this end, two powerful tools are introduced and used: the hypothesis testing operation region and the person-by-person optimality argument. Compared with other analytical methods, the operation region provides an explicit way to characterize a (randomized) decision strategy. A distributed hypothesis testing problem can be reduced to a set of easier problems by using the person-by-person optimality argument. Given an i.i.d. random observation sequence, the asymptotic optimal hypothesis testing performance is shown to be characterized by a Chernoff information in a Bayesian hypothesis test or a Kullback-Leibler divergence in a Neyman-Pearson hypothesis test.

Chapter 3

Privacy-Preserving Distributed Bayesian Hypothesis Test

The physical-layer operation of a class of CPSs, e.g., a sensor network for health monitoring, can be seen as a distributed hypothesis test. The privacy-by-design approach on a such CPS can be realized through a privacy-preserving design of the distributed hypothesis testing network, which realizes not only a good hypothesis testing performance but also a privacy leakage suppression. There are different possible models and measures for the privacy leakage in a distributed hypothesis testing network. Information-theoretic measures, mutual information rate in [44] and Kullback-Leibler divergence in [47], were used to evaluate the privacy leakage. In this chapter, the hypothesis testing performance is measured by the Bayesian risk of fusion decision; the privacy leakage is modeled as a hypothesis test made by an eavesdropper (EVE) based on intercepted remote decisions; and the privacy leakage is measured through the minimal Bayesian risk of eavesdropper decision. Different from the information-theoretic measures, the privacy leakage measure used here has a clear operational meaning. Based on these settings, optimal privacy-preserving distributed hypothesis testing designs are characterized. In particular, the optimality of deterministic likelihood-based test is verified.

3.1 Distributed Hypothesis Test in the Presence of an Eavesdropper

System model

In a CPS application, the communication links between the sensors and the terminal can be open-access or protected. Commonly, a high cost needs to be paid for intercepting the protected messages while messages transmitted through open-access links are vulnerable to eavesdropping. The messages transmitted over the open-access links are modeled as the intercepted remote decisions in the studied

distributed hypothesis testing network in the presence of an EVE.

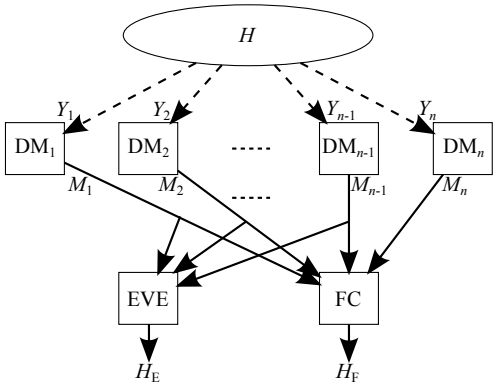


Figure 3.1: A parallel distributed hypothesis testing network in the presence of an EVE. It is shown for illustration that the first $n-1$ remote decisions are intercepted by the EVE. In the discussion, it is considered that the first k, $1 \leq k \leq n$, remote decisions are intercepted.

The studied parallel model in Figure 3.1 consists of an s-ary hypothesis H, n remote decision makers $\{\mathrm{DM}_i\}_{i=1}^n$, an FC, and an EVE. The hypothesis H defined on the alphabet $\mathcal{H} = \{0, \ldots, s-1\}$ is randomly generated following a prior probability distribution p_H. Each remote decision maker DM_i independently makes an s_i-ary remote decision M_i defined on the alphabet $\mathcal{M}_i = \{0, \ldots, s_i - 1\}$ based on the continuous random observation Y_i defined on the alphabet $\mathcal{Y}_i$. The likelihoods of the remote observation Y_i are denoted by $\{f_{Y_i|H}(\cdot|h)\}_{h\in\mathcal{H}}$. All remote observations are assumed to be conditionally independent given a hypothesis h, i.e.,

$$f_{Y^n|H}(y^n|h) = \prod_{i=1}^{n} f_{Y_i|H}(y_i|h). \tag{3.1}$$

All remote decisions are transmitted to the FC through error-free rate-limited links. Based on these remote decisions, the FC makes an s-ary fusion decision H_F to infer the hypothesis H. The EVE is assumed to intercept the first k, $1 \leq k \leq n$, remote decisions M^k and makes an s-ary eavesdropper decision H_E to infer the hypothesis as well. Here, independent (randomized) decision strategies [57] of the $\{\mathrm{DM}_i\}_{i=1}^n$, the FC, and the EVE are denoted by $\{\phi_i\}_{i=1}^n$, ϕ_F, and ϕ_E, respectively:

$$\begin{aligned} \phi_i &: \mathcal{Y}_i \to \mathcal{M}_i,\ 1 \leq i \leq n, \\ \phi_\mathrm{F} &: \mathcal{M}^n \to \mathcal{H}, \\ \phi_\mathrm{E} &: \mathcal{M}^k \to \mathcal{H}. \end{aligned} \tag{3.2}$$

Note that the (randomized) strategies can be equivalently represented by conditional p.m.f.s $\{p_{M_i|Y_i}\}_{i=1}^n$, $p_{H_\mathrm{F}|M^n}$, and $p_{H_\mathrm{E}|M^k}$. Let Φ_i, Φ_F, and Φ_E denote the

(randomized) decision strategy sets of the DM_i, the FC, and the EVE, i.e., $\phi_i \in \Phi_i$, $\phi_{\mathrm{F}} \in \Phi_{\mathrm{F}}$, and $\phi_{\mathrm{E}} \in \Phi_{\mathrm{E}}$. Denote the deterministic strategy subsets by Φ_i^{D}, $\Phi_{\mathrm{F}}^{\mathrm{D}}$, and $\Phi_{\mathrm{E}}^{\mathrm{D}}$, respectively. The cardinalities of the deterministic strategy subsets $\Phi_{\mathrm{F}}^{\mathrm{D}}$ and $\Phi_{\mathrm{E}}^{\mathrm{D}}$ are

$$\begin{aligned} d_{\mathrm{F}} &= \left|\left|\Phi_{\mathrm{F}}^{\mathrm{D}}\right|\right| = s^{\left(\prod_{i=1}^{n} s_i\right)}, \\ d_{\mathrm{E}} &= \left|\left|\Phi_{\mathrm{E}}^{\mathrm{D}}\right|\right| = s^{\left(\prod_{i=1}^{k} s_i\right)}. \end{aligned} \tag{3.3}$$

Informed eavesdropper

In practice, an EVE can be informed, uninformed, or partially informed depending on the EVE status, e.g., an authorized compromised manager of the network or a curious passerby. Here, the EVE is assumed to be informed, i.e., the EVE knows all needed statistics: the prior distribution p_H, the observation likelihoods of the first k intercepted remote decision makers $\{f_{Y_i|H}\}_{i=1}^{k}$, the remote strategies $\{\phi_i\}_{i=1}^{k}$, and the corresponding conditional p.m.f.s $\{p_{M_i|Y_i}\}_{i=1}^{k}$. The assumption of informed EVE means the worst privacy leakage scenario since the statistical knowledge enables the EVE to always choose the best strategy to infer the correct hypothesis. Due to the uncertainty about the status of the EVE, the privacy-preserving design based on the worst privacy leakage scenario leads to a privacy-preserving performance guarantee.

Bayesian privacy leakage measure

Further, there is also an uncertainty about the behavior of the assumed informed EVE, i.e., the privacy leakage model and measure are unknown. For the privacy-by-design approach, the model and measure of privacy leakage follow from the privacy-preserving objective of the system designer. That means the privacy-preserving design needs to be optimized under an assumption of the system designer on the EVE behavior.

In this chapter, the privacy leakage is modeled as a Bayesian hypothesis test made by the informed EVE based on the intercepted remote decisions. The decision costs of the EVE are assigned following the privacy-preserving objective of the system designer and are denoted by $\{c_{\mathrm{E}}(h_{\mathrm{E}}, h)\}_{h_{\mathrm{E}},h\in\mathcal{H}}$. Given a distributed hypothesis testing network design $(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}})$, the privacy leakage is measured by the minimal Bayesian risk of eavesdropper decision:

$$\begin{aligned} r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k) &= \min_{\phi_{\mathrm{E}}\in\Phi_{\mathrm{E}}} \mathrm{E}\left[c_{\mathrm{E}}(H_{\mathrm{E}}, H)\right] \\ &= \min_{\phi_{\mathrm{E}}\in\Phi_{\mathrm{E}}} \int_{\mathcal{Y}^k} \sum_{m^k\in\mathcal{M}^k, h_{\mathrm{E}}, h\in\mathcal{H}} p_{H_{\mathrm{E}}|M^k}(h_{\mathrm{E}}|m^k) \\ &\qquad \prod_{i=1}^{k} p_{M_i|Y_i}(m_i|y_i) f_{Y_i|H}(y_i|h) p_H(h) c_{\mathrm{E}}(h_{\mathrm{E}}, h) dy^k. \end{aligned} \tag{3.4}$$

The EVE makes a centralized Bayesian hypothesis test based on a discrete random observation sequence. Following from a similar analysis on the person-by-person optimization of fusion strategy in (2.25), an optimal eavesdropper strategy is a deterministic likelihood-based test. Therefore, the optimization of ϕ_{E} in (3.4) can be constrained to the deterministic strategy subset $\Phi_{\mathrm{E}}^{\mathrm{D}}$ without loss of optimality, i.e.,

$$\begin{aligned} r_{\mathrm{E}}^{\min}(\phi_1,\ldots,\phi_k) = \min_{\phi_{\mathrm{E}}\in\Phi_{\mathrm{E}}^{\mathrm{D}}} \int_{\mathcal{Y}^k} \sum_{m^k\in\mathcal{M}^k,h_{\mathrm{E}},h\in\mathcal{H}} & p_{H_{\mathrm{E}}|M^k}(h_{\mathrm{E}}|m^k) \\ & \prod_{i=1}^{k} p_{M_i|Y_i}(m_i|y_i) f_{Y_i|H}(y_i|h) p_H(h) c_{\mathrm{E}}(h_{\mathrm{E}},h) dy^k. \end{aligned} \tag{3.5}$$

When the informed EVE is forced to make a decision based on the knowledge of the hypothesis prior distribution only, the worst hypothesis testing performance of the EVE is achieved as:

$$\gamma = \min_{h_{\mathrm{E}}\in\mathcal{H}} \sum_{h\in\mathcal{H}} p_H(h) c_{\mathrm{E}}(h_{\mathrm{E}},h), \tag{3.6}$$

where a term $\sum_{h\in\mathcal{H}} p_H(h) c_{\mathrm{E}}(h_{\mathrm{E}},h)$ corresponds to the Bayesian risk of eavesdropper decision when the EVE always makes a decision $h_{\mathrm{E}} \in \mathcal{H}$ regardless of the intercepted remote decisions, i.e.,

$$H_{\mathrm{E}} = \phi_{\mathrm{E}}(m^k) = h_{\mathrm{E}},\ \forall m^k \in \mathcal{M}^k.$$

Remark 3.1. *The worst hypothesis testing performance of the informed EVE is an upper bound on the privacy leakage measure: For all* $(\phi_1,\ldots,\phi_k) \in \Phi_1 \times \cdots \times \Phi_k$,

$$r_{\mathrm{E}}^{\min}(\phi_1,\ldots,\phi_k) \le \gamma. \tag{3.7}$$

Bayesian hypothesis testing performance measure

The hypothesis testing performance is measured by the Bayesian risk of fusion decision. The decision costs of the FC are denoted by $\{c_{\mathrm{F}}(h_{\mathrm{F}},h)\}_{h_{\mathrm{F}},h\in\mathcal{H}}$. Given a hypothesis testing network design $(\phi_1,\ldots,\phi_n,\phi_{\mathrm{F}})$, the Bayesian risk of fusion decision is:

$$\begin{aligned} r_{\mathrm{F}}(\phi_1,\ldots,\phi_n,\phi_{\mathrm{F}}) &= \mathrm{E}\left[c_{\mathrm{F}}(H_{\mathrm{F}},H)\right] \\ &= \int_{\mathcal{Y}^n} \sum_{m^n\in\mathcal{M}^n,h_{\mathrm{F}},h\in\mathcal{H}} p_{H_{\mathrm{F}}|M^n}(h_{\mathrm{F}}|m^n) \\ &\qquad \prod_{i=1}^{n} p_{M_i|Y_i}(m_i|y_i) f_{Y_i|H}(y_i|h) p_H(h) c_{\mathrm{F}}(h_{\mathrm{F}},h) dy^n. \end{aligned} \tag{3.8}$$

3.2 Privacy-Constrained Distributed Bayesian Test

Problem formulation

Using the Bayesian hypothesis testing performance and privacy leakage measures, the privacy-constrained distributed Bayesian hypothesis testing problem is formulated as

$$\begin{aligned}(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*) = \underset{(\phi_1,\ldots,\phi_n,\phi_{\mathrm{F}})\in\Phi_1\times\cdots\times\Phi_n\times\Phi_{\mathrm{F}}}{\arg\min} \quad & r_{\mathrm{F}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) \\ \text{s.t.} \quad & r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k) \geq \lambda,\end{aligned} \tag{3.9}$$

where λ represents the privacy leakage suppression guarantee. Because of the upper bound on $r_{\mathrm{E}}^{\min}$ in (3.7), the privacy-constrained optimization problem is feasible only if $\lambda \leq \gamma$.

Compared with the distributed Bayesian hypothesis testing problem (2.24), the proposed privacy-constrained problem has the same optimization objective and an additional operational privacy leakage suppression constraint.

Characteristics of an optimal privacy-constrained design

The optimality of deterministic LRT (or likelihood-based test) has been verified for the (distributed) Bayesian hypothesis testing problems. Here, the optimality of deterministic likelihood-based test is to be discussed for the privacy-constrained distributed Bayesian hypothesis testing problem. However, it is difficult to solve (3.9) directly to obtain an optimal privacy-constrained hypothesis testing network design $(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)$. Alternatively, the person-by-person optimality argument can be adopted here: characteristics of a person-by-person optimal privacy-constrained strategy are necessary to be satisfied by an optimal privacy-constrained strategy. That is because an optimal privacy-constrained strategy must be a person-by-person optimal privacy-constrained strategy given other decision strategies in an optimal privacy-constrained distributed hypothesis testing network design.

Theorem 3.1. *For the privacy-constrained Bayesian hypothesis testing problem (3.9), it is sufficient to consider a deterministic likelihood-based test for ϕ_{F}^*.*

Proof. Given an optimal privacy-constrained hypothesis testing network design $(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)$, it follows from the person-by-person optimality argument that

$$\begin{aligned}\phi_{\mathrm{F}}^* = \underset{\phi_{\mathrm{F}}\in\Phi_{\mathrm{F}}}{\arg\min} \; & r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}) \\ \text{s.t.} \quad & r_{\mathrm{E}}^{\min}(\phi_1^*, \ldots, \phi_k^*) \geq \lambda.\end{aligned} \tag{3.10}$$

Since the minimal Bayesian risk of eavesdropper decision does not depend on the fusion strategy, the optimization of ϕ_{F} is not constrained by the privacy leakage

suppression bound. Therefore, the problem (3.10) reduces to a centralized Bayesian hypothesis testing problem:

$$\phi_{\mathrm{F}}^* = \arg\min_{\phi_{\mathrm{F}} \in \Phi_{\mathrm{F}}} r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}).$$

It is sufficient to consider the following deterministic likelihood-based test for ϕ_{F}^*:

$$H_{\mathrm{F}} = \phi_{\mathrm{F}}^*(m^n) = \arg\min_{h_{\mathrm{F}} \in \mathcal{H}} \sum_{h \in \mathcal{H}} p^*_{M^n|H}(m^n|h) p_H(h) c_{\mathrm{F}}(h_{\mathrm{F}}, h), \tag{3.11}$$

where the fusion observation sequence likelihood $p^*_{M^n|H}$ can be expressed in terms of remote observation likelihoods $\{f_{Y_i|H}\}_{i=1}^n$, optimal privacy-constrained remote strategies $(\phi_1^*, \ldots, \phi_n^*)$, and the corresponding conditional p.m.f.s $\{p^*_{M_i|Y_i}\}_{i=1}^n$ as in (2.31). □

Theorem 3.2. *For the privacy-constrained Bayesian hypothesis testing problem (3.9), it is sufficient to consider a deterministic likelihood-based test for ϕ_i^* of a remote decision maker* DM_i *whose decision M_i is not intercepted, i.e., $k{+}1 \leq i \leq n$.*

Proof. Given an optimal privacy-constrained hypothesis testing network design $(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)$, it follows from the person-by-person optimality argument that: For $k+1 \leq i \leq n-1$,

$$\begin{aligned} \phi_i^* = \arg\min_{\phi_i \in \Phi_i} \; & r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_i, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*) \\ \text{s.t.} \quad & r_{\mathrm{E}}^{\min}(\phi_1^*, \ldots, \phi_k^*) \geq \lambda. \end{aligned} \tag{3.12}$$

Since the minimal Bayesian risk of eavesdropper decision does not depend on the remote strategy ϕ_i for $k+1 \leq i \leq n-1$, the optimization of ϕ_{i} is not constrained by the privacy leakage suppression bound. Therefore, the problem (3.12) reduces to the following optimization:

$$\phi_i^* = \arg\min_{\phi_i \in \Phi_i} r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_i, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*).$$

It is sufficient to consider the following deterministic likelihood-based test

$$M_i = \phi_i^*(y_i) = \arg\min_{m_i \in \mathcal{M}_i} \sum_{h \in \mathcal{H}} f_{Y_i|H}(y_i|h) p_H(h) c_i^*(m_i, h), \tag{3.13}$$

where

$$\begin{aligned} c_i^*(m_i, h) \triangleq \int_{\mathcal{Y}^{n\setminus i}} & \sum_{m^{n\setminus i} \in \mathcal{M}^{n\setminus i}, h_{\mathrm{F}} \in \mathcal{H}} p^*_{H_{\mathrm{F}}|M^n}(h_{\mathrm{F}}|m^{n\setminus i}, m_i) \\ & \prod_{j=1, j\neq i}^{n} p^*_{M_j|Y_j}(m_j|y_j) f_{Y_j|H}(y_j|h) c_{\mathrm{F}}(h_{\mathrm{F}}, h) dy^{n\setminus i}. \end{aligned} \tag{3.14}$$

Similarly, an optimal remote strategy ϕ_n^* for the privacy-constrained distributed Bayesian hypothesis testing problem (3.9) is a deterministic likelihood-based test. □

In the following, an optimal privacy-constrained remote strategy ϕ_i^*, $1 \leq i \leq k$, will be characterized. First, the operation region of DM_i is introduced. Since H is an s-ary hypothesis and M_i is an s_i-ary remote decision, a (randomized) remote strategy ϕ_i can be represented by a set of $(s_i - 1) \cdot s$ conditional probabilities, e.g., $\left\{p_{M_i|H}(m_i|h)\right\}_{m_i \in \{1,\ldots,s_i-1\}, h \in \mathcal{H}}$. Denote the operation point achieved by a remote strategy ϕ_i by

$$\boldsymbol{p}_i(\phi_i) \triangleq (p_{M_i|H}(1|0), \ldots, p_{M_i|H}(s_i-1|0), \ldots, p_{M_i|H}(1|s-1), \ldots, p_{M_i|H}(s_i-1|s-1)). \tag{3.15}$$

The operation region of DM_i consists of operation points achieved by all (randomized) remote strategies:

$$\mathcal{R}_i \triangleq \{\boldsymbol{p}_i(\phi_i) | \phi_i \in \Phi_i\}. \tag{3.16}$$

The operation region $\mathcal{R}_i$ has the following properties.

Property 3.1. *Given an s-ary hypothesis H, an s_i-ary remote decision M_i, and a continuous random remote observation Y_i, the $(s_i \cdot s - s)$-dimensional operation region $\mathcal{R}_i$ has the following properties:*

1. *The operation region $\mathcal{R}_i$ is a convex set;*
2. *All operation points on the boundary can be achieved by deterministic likelihood-based tests;*
3. *All inner operation points can be achieved by randomized strategies of two deterministic likelihood-based tests.*

The first property follows from the randomization; the second property can be proved through the method of Lagrange multiplier; and the third property follows from the second property.

Different from the optimality of deterministic likelihood-based test for ϕ_j^* with $k+1 \leq j \leq n$, the following theorem shows that it is not the same case for ϕ_i^* with $1 \leq i \leq k$.

Theorem 3.3. *For the privacy-constrained Bayesian hypothesis testing problem (3.9), an optimal strategy ϕ_i^* of an intercepted remote decision maker DM_i, i.e., $1 \leq i \leq k$, can be a deterministic likelihood-based test or a randomized strategy of two deterministic likelihood-based tests.*

Theorem 3.3 can be proved through the person-by-person optimality argument and the operation region $\mathcal{R}_i$. Since the remote decision M_i is intercepted by the EVE, the privacy leakage suppression constraint takes effect in the following PBPO

problem of ϕ_i: Given an optimal privacy-constrained hypothesis testing network design $(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)$ and for $2 \leq i \leq k-1$,

$$\begin{aligned} \phi_i^* = \arg\min_{\phi_i \in \Phi_i} & \; r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_i, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*) \\ \text{s.t.} & \; r_{\mathrm{E}}^{\min}(\phi_1^*, \ldots, \phi_i, \ldots, \phi_k^*) \geq \lambda. \end{aligned} \tag{3.17}$$

Define

$$\begin{aligned} b_i^*(m_i, h) &\triangleq (c_i^*(m_i, h) - c_i^*(0, h)) p_H(h), \\ b_i^* &\triangleq \sum_{h \in \mathcal{H}} c_i^*(0, h) p_H(h), \end{aligned} \tag{3.18}$$

where $c_i^*(m_i, h)$ is defined in (3.14). The Bayesian risk $r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_i, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)$ can be expressed as an affine function of $\boldsymbol{p}_i(\phi_i)$ as

$$\begin{aligned} r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_i, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*) &= \sum_{m_i \in \{1, \ldots, s_i - 1\}, h \in \mathcal{H}} b_i^*(m_i, h) p_{M_i|H}(m_i|h) + b_i^* \\ &= \boldsymbol{b}_i^* \boldsymbol{p}_i^\top(\phi_i) + b_i^*, \end{aligned} \tag{3.19}$$

where the coefficient vector is $\boldsymbol{b}_i^* \triangleq (b_i^*(1, 0), \ldots, b_i^*(s_i - 1, s - 1))$.

The privacy leakage suppression constraint $r_{\mathrm{E}}^{\min}(\phi_1^*, \ldots, \phi_i, \ldots, \phi_k^*) \geq \lambda$ means that $r_{\mathrm{E}}(\phi_1^*, \ldots, \phi_i, \ldots, \phi_k^*, \phi_{\mathrm{E}}) \geq \lambda$ for all $\phi_{\mathrm{E}} \in \Phi_{\mathrm{E}}$. The previous analysis has shown that it is sufficient to consider deterministic eavesdropper strategies. Therefore, the privacy leakage suppression constraint can further be rewritten as

$$\begin{gathered} r_{\mathrm{E}}^{\min}(\phi_1^*, \ldots, \phi_i, \ldots, \phi_k^*) \geq \lambda \\ \Updownarrow \\ r_{\mathrm{E}}(\phi_1^*, \ldots, \phi_i, \ldots, \phi_k^*, \phi_{\mathrm{E}}) \geq \lambda, \text{ for all } \phi_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}. \end{gathered} \tag{3.20}$$

Given an eavesdropper strategy $\phi_{\mathrm{E}} \in \Phi_{\mathrm{E}}$, $r_{\mathrm{E}}(\phi_1^*, \ldots, \phi_i, \ldots, \phi_k^*, \phi_{\mathrm{E}})$ is also an affine function of $\boldsymbol{p}_i(\phi_i)$ as

$$\begin{aligned} r_{\mathrm{E}}(\phi_1^*, \ldots, \phi_i, \ldots, \phi_k^*, \phi_{\mathrm{E}}) &= \sum_{m_i \in \{1, \ldots, s_i - 1\}, h \in \mathcal{H}} b_i^*(\phi_{\mathrm{E}}, m_i, h) p_{M_i|H}(m_i|h) + b_i^*(\phi_{\mathrm{E}}) \\ &= \boldsymbol{b}_i^*(\phi_{\mathrm{E}}) \boldsymbol{p}_i^\top(\phi_i) + b_i^*(\phi_{\mathrm{E}}), \end{aligned} \tag{3.21}$$

where

$$\begin{aligned}
\boldsymbol{b}_i^*(\phi_{\mathrm{E}}) &\triangleq (b_i^*(\phi_{\mathrm{E}},1,0),\ldots,b_i^*(\phi_{\mathrm{E}},s_i-1,s-1));\\
b_i^*(\phi_{\mathrm{E}},m_i,h) &\triangleq (c_i^*(\phi_{\mathrm{E}},m_i,h)-c_i^*(\phi_{\mathrm{E}},0,h))p_H(h);\\
b_i^*(\phi_{\mathrm{E}}) &\triangleq \sum_{h\in\mathcal{H}} c_i^*(\phi_{\mathrm{E}},0,h)p_H(h);\\
c_i^*(\phi_{\mathrm{E}},m_i,h) &\triangleq \int_{\mathcal{Y}^{k\setminus i}} \sum_{m^{k\setminus i}\in\mathcal{M}^{k\setminus i},h_{\mathrm{E}}\in\mathcal{H}} p_{H_{\mathrm{E}}|M^k}(h_{\mathrm{E}}|m^{k\setminus i},m_i)\\
&\qquad \prod_{j=1,j\neq i}^{k} p^*_{M_j|Y_j}(m_j|y_j)f_{Y_j|H}(y_j|h)c_{\mathrm{E}}(h_{\mathrm{E}},h)dy^{k\setminus i}.
\end{aligned} \tag{3.22}$$

The problem in (3.17) can be equivalently rewritten as

$$\begin{aligned}
\phi_i^* = \arg\min_{\phi_i\in\Phi_i}\ & \boldsymbol{b}_i^*\boldsymbol{p}_i^\top(\phi_i)+b_i^*\\
\text{s.t.}\quad & \boldsymbol{b}_i^*(\phi_{\mathrm{E}})\boldsymbol{p}_i^\top(\phi_i)+b_i^*(\phi_{\mathrm{E}})\geq\lambda,\ \forall\phi_{\mathrm{E}}\in\Phi_{\mathrm{E}}^{\mathrm{D}}.
\end{aligned} \tag{3.23}$$

Given a deterministic eavesdropper strategy $\phi_{\mathrm{E}}\in\Phi_{\mathrm{E}}^{\mathrm{D}}$, define a privacy constraint region $\mathcal{P}_i(\phi_{\mathrm{E}})$ and its privacy constraint hyperplane $\partial\mathcal{P}_i(\phi_{\mathrm{E}})$ as

$$\begin{aligned}
\mathcal{P}_i(\phi_{\mathrm{E}}) &\triangleq \left\{\boldsymbol{p}_i(\phi_i)\,\middle|\,\boldsymbol{b}_i^*(\phi_{\mathrm{E}})\boldsymbol{p}_i^\top(\phi_i)+b_i^*(\phi_{\mathrm{E}})\geq\lambda\right\},\\
\partial\mathcal{P}_i(\phi_{\mathrm{E}}) &\triangleq \left\{\boldsymbol{p}_i(\phi_i)\,\middle|\,\boldsymbol{b}_i^*(\phi_{\mathrm{E}})\boldsymbol{p}_i^\top(\phi_i)+b_i^*(\phi_{\mathrm{E}})=\lambda\right\}.
\end{aligned} \tag{3.24}$$

Then, the privacy-constrained operation region $\mathcal{R}_i^{\mathrm{P}}$ of the intercepted DM_i is defined as

$$\mathcal{R}_i^{\mathrm{P}} \triangleq \left\{\bigcap_{\phi_{\mathrm{E}}\in\Phi_{\mathrm{E}}^{\mathrm{D}}}\mathcal{P}_i(\phi_{\mathrm{E}})\right\}\cap\mathcal{R}_i. \tag{3.25}$$

Since $\mathcal{R}_i$ and $\{\mathcal{P}_i(\phi_{\mathrm{E}})\}_{\phi_{\mathrm{E}}\in\Phi_{\mathrm{E}}^{\mathrm{D}}}$ are convex sets, $\mathcal{R}_i^{\mathrm{P}}$ is a convex set [8]. An illustration of $\mathcal{R}_i^{\mathrm{P}}$ is shown in Figure 3.2. The PBPO problem (3.23) is to find an optimal operation point $\boldsymbol{p}_i(\phi_i^*)$ which minimizes the affine objective function $\boldsymbol{b}_i^*\boldsymbol{p}_i^\top(\phi_i)+b_i^*$ in the convex privacy-constrained operation region $\mathcal{R}_i^{\mathrm{P}}$. Then, the following lemma follows from the convex optimization theory.

Lemma 3.1. *From [8], an optimal operation point of the problem (3.23) is on the boundary of the privacy-constrained operation region $\mathcal{R}_i^{\mathrm{P}}$ and has a supporting hyperplane in parallel with the objective function hyperplane $\boldsymbol{b}_i^*\boldsymbol{p}_i^\top(\phi_i)+b_i^*$.*

Based on Lemma 3.1, Theorem 3.3 can easily be proved as follows.

Proof. Two distinct parts can be identified on the boundary $\partial\mathcal{R}_i^{\mathrm{P}}$ as: $\partial\mathcal{R}_i^{\mathrm{P}}\cap\partial\mathcal{R}_i$, $\bigcup_{\phi_{\mathrm{E}}\in\Phi_{\mathrm{E}}^{\mathrm{D}}}\left\{\partial\mathcal{R}_i^{\mathrm{P}}\cap\partial\mathcal{P}_i(\phi_{\mathrm{E}})\right\}$. If an optimal operation point of the problem (3.23)

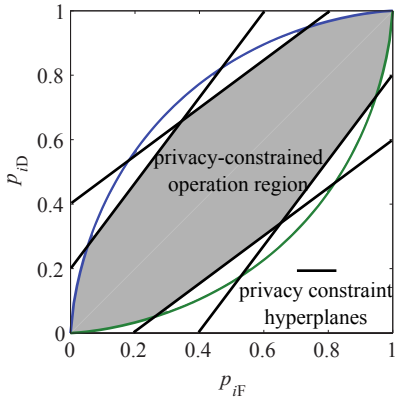


Figure 3.2: A privacy-constrained operation region $\mathcal{R}_i^{\mathrm{P}}$ of an intercepted remote decision maker DM_i when the hypothesis H and the remote decision M_i are both binary random variables; the continuous random observation Y_i is generated following $Y_i|H = 0 \sim \mathcal{N}(0,1)$ or $Y_i|H = 1 \sim \mathcal{N}(1,1)$; and there are four privacy constraint regions taking effect.

is on $\partial\mathcal{R}_i^{\mathrm{P}} \cap \partial\mathcal{R}_i$, Property 3.1 of $\mathcal{R}_i$ implies that an optimal remote strategy of the problem (3.23) is a deterministic likelihood-based test. Otherwise, an optimal operation point is on the hyperplanes $\bigcup_{\phi_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}} \left\{\partial\mathcal{R}_i^{\mathrm{P}} \cap \partial\mathcal{P}_i(\phi_{\mathrm{E}})\right\}$ or sufficiently is an intersection of the hyperplanes. In this case, an optimal operation point of the problem (3.23) is in the following intersection set

$$\bigcup_{\phi_{\mathrm{E}}, \phi'_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}, \phi_{\mathrm{E}} \neq \phi'_{\mathrm{E}}} \left\{\partial\mathcal{R}_i^{\mathrm{P}} \cap \partial\mathcal{P}_i(\phi_{\mathrm{E}}) \cap \partial\mathcal{P}_i(\phi'_{\mathrm{E}})\right\}; \tag{3.26}$$

and Property 3.1 of $\mathcal{R}_i$ implies that an optimal remote strategy of the problem (3.23) is a randomized strategy of two deterministic likelihood-based tests. The above analysis justifies Theorem 3.3 for an intercepted remote decision maker DM_i with $2 \leq i \leq k-1$. Similarly, Theorem 3.3 also holds for intercepted DM_1 or DM_k. □

Remark 3.2. *If an optimal remote strategy of the problem (3.23) is a randomized decision strategy of two deterministic likelihood-based tests, this optimal remote strategy is determined by the privacy constraint condition only.*

Extended PBPO algorithm

A PBPO algorithm can be used to design an optimal distributed Bayesian hypothesis testing network. Based on the obtained characteristics, an extended PBPO al-

gorithm is proposed to design an optimal privacy-constrained distributed Bayesian hypothesis testing network.

Give a distributed hypothesis testing network design $(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}})$ which satisfies the privacy leakage suppression constraint as $r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k) \geq \lambda$. The hypothesis testing performance can be improved through a PBPO of a decision strategy while the other given strategies are fixed.

Denote a person-by-person optimal fusion strategy by $\phi_{\mathrm{F}}^{\Delta}$. From Theorem 3.1, it is sufficient to consider the following deterministic likelihood-based test for $\phi_{\mathrm{F}}^{\Delta}$:

$$H_{\mathrm{F}} = \phi_{\mathrm{F}}^{\Delta}(m^n) = \arg\min_{h_{\mathrm{F}} \in \mathcal{H}} \sum_{h \in \mathcal{H}} p_{M^n|H}(m^n|h) p_H(h) c_{\mathrm{F}}(h_{\mathrm{F}}, h), \tag{3.27}$$

where the fusion observation sequence likelihood $p_{M^n|H}$ can be expressed in terms of remote observation likelihoods $\{f_{Y_i|H}\}_{i=1}^n$, the fixed remote strategies $(\phi_1, \ldots, \phi_n)$, and the corresponding conditional p.m.f.s $\{p_{M_i|Y_i}\}_{i=1}^n$ as in (2.31).

For any $k+1 \leq i \leq n$, the remote decision maker DM_i is not intercepted. Denote a person-by-person optimal remote strategy by ϕ_i^{Δ}. From Theorem 3.2, it is sufficient to consider the following deterministic likelihood-based test for ϕ_i^{Δ}:

$$M_i = \phi_i^{\Delta}(y_i) = \arg\min_{m_i \in \mathcal{M}_i} \sum_{h \in \mathcal{H}} f_{Y_i|H}(y_i|h) p_H(h) c_i(m_i, h), \tag{3.28}$$

where

$$\begin{aligned} c_i(m_i, h) \triangleq \int_{\mathcal{Y}^{n\setminus i}} & \sum_{m^{n\setminus i} \in \mathcal{M}^{n\setminus i}, h_{\mathrm{F}} \in \mathcal{H}} p_{H_{\mathrm{F}}|M^n}(h_{\mathrm{F}}|m^{n\setminus i}, m_i) \\ & \prod_{j=1, j\neq i}^{n} p_{M_j|Y_j}(m_j|y_j) f_{Y_j|H}(y_j|h) c_{\mathrm{F}}(h_{\mathrm{F}}, h) dy^{n\setminus i}. \end{aligned} \tag{3.29}$$

For any $1 \leq i \leq k$, the remote decision maker DM_i is intercepted. Denote a person-by-person optimal remote strategy by ϕ_i^{Δ}. Following a similar proof as Theorem 3.3, it can be shown that a person-by-person optimal remote strategy ϕ_i^{Δ} of intercepted DM_i can be a deterministic likelihood-based test or a randomized strategy of two deterministic likelihood-based tests. Given deterministic eavesdropper strategy $\phi_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}$, define the person-by-person privacy constraint region $\mathcal{P}_i^{\Delta}(\phi_{\mathrm{E}})$ and its person-by-person privacy constraint hyperplane $\partial\mathcal{P}_i^{\Delta}(\phi_{\mathrm{E}})$ similarly as (3.24) as

$$\begin{aligned} \mathcal{P}_i^{\Delta}(\phi_{\mathrm{E}}) &\triangleq \left\{ \boldsymbol{p}_i(\phi_i) \,\middle|\, \boldsymbol{b}_i(\phi_{\mathrm{E}}) \boldsymbol{p}_i^{\top}(\phi_i) + b_i(\phi_{\mathrm{E}}) \geq \lambda \right\}, \\ \partial\mathcal{P}_i^{\Delta}(\phi_{\mathrm{E}}) &\triangleq \left\{ \boldsymbol{p}_i(\phi_i) \,\middle|\, \boldsymbol{b}_i(\phi_{\mathrm{E}}) \boldsymbol{p}_i^{\top}(\phi_i) + b_i(\phi_{\mathrm{E}}) = \lambda \right\}, \end{aligned}$$

where

$$\boldsymbol{b}_i(\phi_{\mathrm{E}}) \triangleq (b_i(\phi_{\mathrm{E}},1,0),\ldots,b_i(\phi_{\mathrm{E}},s_i-1,s-1));$$
$$b_i(\phi_{\mathrm{E}},m_i,h) \triangleq (c_i(\phi_{\mathrm{E}},m_i,h)-c_i(\phi_{\mathrm{E}},0,h))p_H(h);$$
$$b_i(\phi_{\mathrm{E}}) \triangleq \sum_{h\in\mathcal{H}} c_i(\phi_{\mathrm{E}},0,h)p_H(h);$$
$$c_i(\phi_{\mathrm{E}},m_i,h) \triangleq \int_{\mathcal{Y}^{k\setminus i}} \sum_{m^{k\setminus i}\in\mathcal{M}^{k\setminus i},h_{\mathrm{E}}\in\mathcal{H}} p_{H_{\mathrm{E}}|M^k}(h_{\mathrm{E}}|m^{k\setminus i},m_i) \prod_{j=1,j\neq i}^{k} p_{M_j|Y_j}(m_j|y_j)f_{Y_j|H}(y_j|h)c_{\mathrm{E}}(h_{\mathrm{E}},h)dy^{k\setminus i}.$$

The person-by-person privacy-constrained operation region $\mathcal{R}_i^{\mathrm{P}\Delta}$ is similarly defined in terms of $\left\{\mathcal{P}_i^{\Delta}(\phi_{\mathrm{E}})\right\}_{\phi_{\mathrm{E}}\in\Phi_{\mathrm{E}}^{\mathrm{D}}}$ as (3.25) as

$$\mathcal{R}_i^{\mathrm{P}\Delta} \triangleq \left\{\bigcap_{\phi_{\mathrm{E}}\in\Phi_{\mathrm{E}}^{\mathrm{D}}} \mathcal{P}_i^{\Delta}(\phi_{\mathrm{E}})\right\} \cap \mathcal{R}_i.$$

The standard PBPO can be extended as:

1. A person-by-person optimal remote strategy ϕ_i^{Δ} of intercepted DM_i is the deterministic likelihood-based test in (3.28) if the privacy leakage suppression constraint is satisfied as $r_{\mathrm{E}}^{\min}(\phi_1,\ldots,\phi_i^{\Delta},\ldots,\phi_k) \geq \lambda$;
2. Otherwise, search a person-by-person optimal remote strategy ϕ_i^{Δ} of intercepted DM_i through deterministic likelihood-based tests which achieve operation points in the set $\bigcup_{\phi_{\mathrm{E}}\in\Phi_{\mathrm{E}}^{\mathrm{D}}} \left\{\partial\mathcal{R}_i^{\mathrm{P}\Delta} \cap \partial\mathcal{R}_i \cap \partial\mathcal{P}_i^{\Delta}(\phi_{\mathrm{E}})\right\}$ and randomized strategies of two deterministic likelihood-based tests which achieve operation points in the following person-by-person privacy constraint hyperplane intersection set $\bigcup_{\phi_{\mathrm{E}},\phi'_{\mathrm{E}}\in\Phi_{\mathrm{E}}^{\mathrm{D}},\phi_{\mathrm{E}}\neq\phi'_{\mathrm{E}}} \left\{\partial\mathcal{R}_i^{\mathrm{P}\Delta} \cap \partial\mathcal{P}_i^{\Delta}(\phi_{\mathrm{E}}) \cap \partial\mathcal{P}_i^{\Delta}(\phi'_{\mathrm{E}})\right\}$. Linear programming methods [6] can be used to search through the person-by-person privacy constraint hyperplane intersections.

Algorithm 3.1 in the appendix of this chapter is the extended PBPO algorithm to design an optimal privacy-constrained distributed Bayesian hypothesis testing network.

3.3 Privacy-Concerned Distributed Bayesian Test

The privacy-constrained problem guarantees an absolute privacy leakage suppression level and optimizes the hypothesis testing performance. A different privacy-preserving idea is to balance both objectives of improving the hypothesis testing performance and suppressing the privacy leakage with different weights. This idea leads to the following privacy-concerned problem.

Problem formulation

Using the Bayesian hypothesis testing privacy leakage and performance measures in (3.5) and (3.8), the privacy-concerned distributed Bayesian hypothesis testing problem is formulated as follows. Given $0 < \eta \leq 1$,

$$\begin{aligned}&(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)\\ =& \underset{(\phi_1,\ldots,\phi_n,\phi_{\mathrm{F}})\in\Phi_1\times\cdots\times\Phi_n\times\Phi_{\mathrm{F}}}{\arg\min} \eta r_{\mathrm{F}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) - (1-\eta) r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k),\end{aligned} \tag{3.30}$$

where η represents the concern weight of improving hypothesis testing performance, i.e., minimizing the Bayesian risk of fusion decision, and $1-\eta$ represents the concern weight of suppressing privacy leakage, i.e., maximizing the minimal Bayesian risk of eavesdropper decision. In this general formulation, the weight η cannot be set to be 0. Otherwise, if not all remote decisions are intercepted, i.e., $k \neq n$, the privacy-concerned optimization problem does not lead to a complete design of the distributed hypothesis testing network. When η decreases, more concern is put on suppressing the privacy leakage. On the contrary, more concern is put on improving the hypothesis testing performance with an increasing weight η.

Characteristics of an optimal privacy-concerned design

Similar to the study on the privacy-constrained distributed Bayesian hypothesis testing problem, it is difficult to solve (3.30) directly to obtain an optimal privacy-concerned distributed hypothesis testing network design $(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)$. Again, the properties of an optimal privacy-concerned distributed hypothesis testing network design are analyzed based on the person-by-person optimality argument that properties of a person-by-person optimal privacy-concerned strategy are necessary to be satisfied by an optimal privacy-concerned strategy.

Theorem 3.4. *For the privacy-concerned Bayesian hypothesis testing problem (3.30), it is sufficient to consider a deterministic likelihood-based test for ϕ_{F}^*.*

Proof. Given an optimal privacy-concerned network design $(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)$, it follows from the person-by-person optimality argument that

$$\phi_{\mathrm{F}}^* = \underset{\phi_{\mathrm{F}}\in\Phi_{\mathrm{F}}}{\arg\min}\, \eta r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}) - (1-\eta) r_{\mathrm{E}}^{\min}(\phi_1^*, \ldots, \phi_k^*). \tag{3.31}$$

Since the minimal Bayesian risk of eavesdropper decision does not depend on the fusion strategy, the second weighted term $-(1-\eta) r_{\mathrm{E}}^{\min}(\phi_1^*, \ldots, \phi_k^*)$ is fixed. Therefore, the problem (3.31) reduces to a centralized Bayesian hypothesis testing problem:

$$\phi_{\mathrm{F}}^* = \underset{\phi_{\mathrm{F}}\in\Phi_{\mathrm{F}}}{\arg\min}\, r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}).$$

It is sufficient to consider the deterministic likelihood-based test in (3.11) for ϕ_{F}^*. □

Theorem 3.5. *For the privacy-concerned Bayesian hypothesis testing problem (3.30), it is sufficient to consider a deterministic likelihood-based test for ϕ_i^* of a remote decision maker* DM_i *whose remote decision M_i is not intercepted, i.e., $k+1 \leq i \leq n$.*

Proof. Given an optimal privacy-concerned network design $(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)$, it follows from the person-by-person optimality argument that: For $k+1 \leq i \leq n-1$,

$$\phi_i^* = \arg\min_{\phi_i \in \Phi_i} \eta r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_i, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*) - (1-\eta) r_{\mathrm{E}}^{\min}(\phi_1^*, \ldots, \phi_k^*). \tag{3.32}$$

Since the minimal Bayesian risk of eavesdropper decision does not depend on the remote strategy ϕ_i for $k+1 \leq i \leq n-1$, the second weighted term $-(1-\eta) r_{\mathrm{E}}^{\min}(\phi_1^*, \ldots, \phi_k^*)$ is fixed. Therefore, the problem (3.32) reduces to the following optimization:

$$\phi_i^* = \arg\min_{\phi_i \in \Phi_i} r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_i, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*).$$

It is sufficient to consider the deterministic likelihood-based test in (3.13).

Similarly, an optimal remote strategy ϕ_n^* for the privacy-concerned distributed Bayesian hypothesis testing problem (3.30) is a deterministic likelihood-based test. □

In the following, an optimal privacy-concerned remote strategy ϕ_i^* of an intercepted remote decision maker DM_i, i.e., $1 \leq i \leq k$, is to be characterized. Different from the optimality of deterministic likelihood-based test for ϕ_j^* with $k+1 \leq j \leq n$, the following theorem shows that it is not the same case for ϕ_i^* with $1 \leq i \leq k$.

Theorem 3.6. *For the privacy-concerned Bayesian hypothesis testing problem (3.30), an optimal remote strategy ϕ_i^* of an intercepted remote decision maker* DM_i*, i.e., $1 \leq i \leq k$, can be a deterministic likelihood-based test or a randomized strategy of two deterministic likelihood-based tests.*

Theorem 3.6 can be proved through the person-by-person optimality argument and the operation region $\mathcal{R}_i$. Since the remote decision M_i is intercepted by the EVE, the second weighted term takes effect in the following PBPO problem of ϕ_i: Given an optimal privacy-concerned hypothesis testing network design $(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)$ and for $2 \leq i \leq k-1$,

$$\phi_i^* = \arg\min_{\phi_i \in \Phi_i} \eta r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_i, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*) - (1-\eta) r_{\mathrm{E}}^{\min}(\phi_1^*, \ldots, \phi_i, \ldots, \phi_k^*). \tag{3.33}$$

The Bayesian risk $r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_i, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)$ can be expressed as the affine function of operation point $\boldsymbol{p}_i(\phi_i)$ in (3.19). Given an eavesdropper strategy $\phi_{\mathrm{E}} \in \Phi_{\mathrm{E}}$, $r_{\mathrm{E}}(\phi_1^*, \ldots, \phi_i, \ldots, \phi_k^*, \phi_{\mathrm{E}})$ can be represented as the affine function of $\boldsymbol{p}_i(\phi_i)$ in (3.21). However, the optimization objective function of ϕ_i in (3.33) cannot be specified since the optimal eavesdropper strategy depends on the optimization argument ϕ_i. In the following, the privacy concern regions are introduced and the

problem (3.33) is to be divided into a set of optimization problems where the objective functions of ϕ_i can be specified.

Given two different deterministic eavesdropper strategies ϕ_{E}, $\phi'_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}$, define a privacy concern halfspace $\mathcal{C}_i(\phi_{\mathrm{E}}, \phi'_{\mathrm{E}})$ and its privacy concern hyperplane $\partial\mathcal{C}_i(\phi_{\mathrm{E}}, \phi'_{\mathrm{E}})$ as

$$\begin{aligned}\mathcal{C}_i(\phi_{\mathrm{E}}, \phi'_{\mathrm{E}}) &\triangleq \left\{\boldsymbol{p}_i(\phi_i) \,\middle|\, \boldsymbol{b}_i^*(\phi_{\mathrm{E}})\boldsymbol{p}_i^{\top}(\phi_i) + b_i^*(\phi_{\mathrm{E}}) \leq \boldsymbol{b}_i^*(\phi'_{\mathrm{E}})\boldsymbol{p}_i^{\top}(\phi_i) + b_i^*(\phi'_{\mathrm{E}})\right\},\\ \partial\mathcal{C}_i(\phi_{\mathrm{E}}, \phi'_{\mathrm{E}}) &\triangleq \left\{\boldsymbol{p}_i(\phi_i) \,\middle|\, \boldsymbol{b}_i^*(\phi_{\mathrm{E}})\boldsymbol{p}_i^{\top}(\phi_i) + b_i^*(\phi_{\mathrm{E}}) = \boldsymbol{b}_i^*(\phi'_{\mathrm{E}})\boldsymbol{p}_i^{\top}(\phi_i) + b_i^*(\phi'_{\mathrm{E}})\right\}.\end{aligned} \tag{3.34}$$

Given a deterministic eavesdropper strategy $\phi_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}$, a privacy concern region $\mathcal{R}_i(\phi_{\mathrm{E}})$ is defined as

$$\mathcal{R}_i(\phi_{\mathrm{E}}) \triangleq \left\{\bigcap_{\phi'_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}, \phi'_{\mathrm{E}} \neq \phi_{\mathrm{E}}} \mathcal{C}_i(\phi_{\mathrm{E}}, \phi'_{\mathrm{E}})\right\} \cap \mathcal{R}_i. \tag{3.35}$$

Remark 3.3. *If a remote strategy ϕ_i which achieves an operation point $\boldsymbol{p}_i(\phi_i) \in \mathcal{R}_i(\phi_{\mathrm{E}})$ is used, then an optimal eavesdropper strategy is the deterministic strategy $\phi_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}$.*

Property 3.2. *The privacy concern region $\mathcal{R}_i(\phi_{\mathrm{E}})$ has the following properties:*

1. *$\mathcal{R}_i(\phi_{\mathrm{E}})$ is a convex set;*
2. *$\bigcup_{\phi_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}} \mathcal{R}_i(\phi_{\mathrm{E}}) = \mathcal{R}_i$.*

The first property follows since intersection is a convexity-preserving operation. The second property follows from fundamental laws of set algebra.

Therefore, the operation region $\mathcal{R}_i$ of an intercepted remote decision maker DM_i can be divided into convex privacy concern regions. Figure 3.3 illustrates the divisions of $\mathcal{R}_i$.

Based on Remark 3.3, Theorem 3.6 is proved as follows.

Proof. The PBPO problem (3.33) can be rewritten as

$$\phi_i^* = \min_{\phi_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}} \; \arg\min_{\{\phi_i | \boldsymbol{p}_i(\phi_i) \in \mathcal{R}_i(\phi_{\mathrm{E}})\}} \eta(\boldsymbol{b}_i^*\boldsymbol{p}_i^{\top}(\phi_i) + b_i^*) - (1-\eta)(\boldsymbol{b}_i^*(\phi_{\mathrm{E}})\boldsymbol{p}_i^{\top}(\phi_i) + b_i^*(\phi_{\mathrm{E}})). \tag{3.36}$$

Given $\phi_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}$, the inner optimization of (3.36) is to minimize an affine function of $\boldsymbol{p}_i(\phi_i)$ over a convex privacy concern region $\mathcal{R}_i(\phi_{\mathrm{E}})$. Therefore, an optimal operation point of the inner minimization is on the boundary $\partial\mathcal{R}_i(\phi_{\mathrm{E}})$. If an inner optimal operation point is on $\partial\mathcal{R}_i(\phi_{\mathrm{E}}) \cap \partial\mathcal{R}_i$, an inner optimal remote strategy is a deterministic likelihood-based test based on Property 3.1 of $\mathcal{R}_i$. Otherwise, an inner optimal operation point is on the hyperplanes $\bigcup_{\phi'_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}, \phi'_{\mathrm{E}} \neq \phi_{\mathrm{E}}} \{\partial\mathcal{R}_i(\phi_{\mathrm{E}}) \cap$

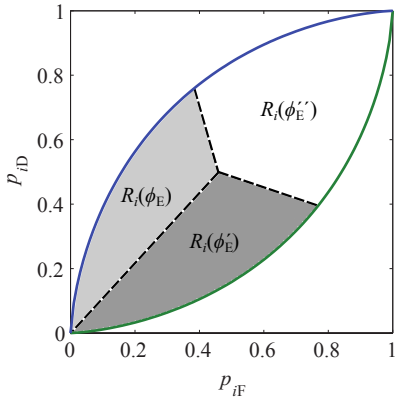


Figure 3.3: Illustration of divisions of the operation region $\mathcal{R}_i$ of an intercepted remote decision maker DM_i when the hypothesis H and the remote decision M_i are both binary random variables; the continuous random observation Y_i is generated following $Y_i|H = 0 \sim \mathcal{N}(0,1)$ or $Y_i|H = 1 \sim \mathcal{N}(1,1)$; and there are three privacy concern regions corresponding to deterministic eavesdropper strategies $\mathcal{R}_i(\phi_\mathrm{E})$, $\mathcal{R}_i(\phi_\mathrm{E}')$, $\mathcal{R}_i(\phi_\mathrm{E}'')$.

$\partial\mathcal{C}_i(\phi_\mathrm{E}, \phi_\mathrm{E}')\}$ or sufficiently is an intersection of the privacy concern hyperplanes in the following set:

$$\bigcup_{\substack{\phi_\mathrm{E}', \phi_\mathrm{E}'' \in \Phi_\mathrm{E}^\mathrm{D} \\ \phi_\mathrm{E}' \neq \phi_\mathrm{E}, \phi_\mathrm{E}'' \neq \phi_\mathrm{E}, \phi_\mathrm{E}' \neq \phi_\mathrm{E}''}} \{\partial\mathcal{R}_i(\phi_\mathrm{E}) \cap \partial\mathcal{C}_i(\phi_\mathrm{E}, \phi_\mathrm{E}') \cap \partial\mathcal{C}_i(\phi_\mathrm{E}, \phi_\mathrm{E}'')\}\,. \tag{3.37}$$

In this case, an inner optimal remote strategy is a randomized strategy of two deterministic likelihood-based tests. Since the inner optimal remote strategies are candidates for an optimal privacy-concerned remote strategy of the PBPO problem (3.36), it can be concluded that an optimal privacy-concerned remote strategy ϕ_i^* achieves an operation point on the boundary $\partial\mathcal{R}_i$ or in the following intersection set:

$$\bigcup_{\substack{\phi_\mathrm{E}, \phi_\mathrm{E}', \phi_\mathrm{E}'' \in \Phi_\mathrm{E}^\mathrm{D} \\ \phi_\mathrm{E}' \neq \phi_\mathrm{E}, \phi_\mathrm{E}'' \neq \phi_\mathrm{E}, \phi_\mathrm{E}' \neq \phi_\mathrm{E}''}} \{\partial\mathcal{R}_i(\phi_\mathrm{E}) \cap \partial\mathcal{C}_i(\phi_\mathrm{E}, \phi_\mathrm{E}') \cap \partial\mathcal{C}_i(\phi_\mathrm{E}, \phi_\mathrm{E}'')\}\,. \tag{3.38}$$

Therefore, Theorem 3.6 is verified that an optimal privacy-concerned strategy ϕ_i^* of an intercepted remote decision maker DM_i can be a deterministic likelihood-based test or a randomized decision strategy of two deterministic likelihood-based tests. □

Extended PBPO algorithm

An extended PBPO algorithm has been proposed to design an optimal privacy-constrained distributed Bayesian hypothesis testing network. Based on the obtained characteristics, another extended PBPO algorithm is proposed to design an optimal privacy-concerned distributed Bayesian hypothesis testing network.

Give a distributed hypothesis testing network design $(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}})$. The weighted sum measure of hypothesis testing performance and privacy leakage can be improved through a PBPO of a decision strategy while the other given strategies are fixed.

Denote a person-by-person optimal fusion strategy by $\phi_{\mathrm{F}}^{\Delta}$. From Theorem 3.4, it is sufficient to consider the deterministic likelihood-based test in (3.27) for $\phi_{\mathrm{F}}^{\Delta}$.

For any $k+1 \leq i \leq n$, the remote decision maker DM_i is not intercepted. Denote a person-by-person optimal remote strategy by ϕ_i^{Δ}. From Theorem 3.5, it is sufficient to consider the deterministic likelihood-based test in (3.28) for ϕ_i^{Δ}.

For any $1 \leq i \leq k$, the remote decision maker DM_i is intercepted. Denote a person-by-person optimal remote strategy by ϕ_i^{Δ}. Following a similar proof as Theorem 3.6, it can be shown that a person-by-person optimal remote strategy ϕ_i^{Δ} of intercepted DM_i can be a deterministic likelihood-based test or a randomized strategy of two deterministic likelihood-based tests. Given two different deterministic eavesdropper strategies ϕ_{E}, $\phi'_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}$, define the person-by-person privacy concern halfspace $\mathcal{C}_i^{\Delta}(\phi_{\mathrm{E}}, \phi'_{\mathrm{E}})$ and its person-by-person privacy concern hyperplane $\partial\mathcal{C}_i^{\Delta}(\phi_{\mathrm{E}}, \phi'_{\mathrm{E}})$ similarly as (3.34) as

$$\begin{aligned}
\mathcal{C}_i^{\Delta}(\phi_{\mathrm{E}}, \phi'_{\mathrm{E}}) &\triangleq \left\{ \boldsymbol{p}_i(\phi_i) \,\middle|\, \boldsymbol{b}_i(\phi_{\mathrm{E}}) \boldsymbol{p}_i^{\top}(\phi_i) + b_i(\phi_{\mathrm{E}}) \leq \boldsymbol{b}_i(\phi'_{\mathrm{E}}) \boldsymbol{p}_i^{\top}(\phi_i) + b_i(\phi'_{\mathrm{E}}) \right\}, \\
\partial\mathcal{C}_i^{\Delta}(\phi_{\mathrm{E}}, \phi'_{\mathrm{E}}) &\triangleq \left\{ \boldsymbol{p}_i(\phi_i) \,\middle|\, \boldsymbol{b}_i(\phi_{\mathrm{E}}) \boldsymbol{p}_i^{\top}(\phi_i) + b_i(\phi_{\mathrm{E}}) = \boldsymbol{b}_i(\phi'_{\mathrm{E}}) \boldsymbol{p}_i^{\top}(\phi_i) + b_i(\phi'_{\mathrm{E}}) \right\}.
\end{aligned}$$

Given a deterministic eavesdropper strategy $\phi_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}$, the person-by-person privacy concern region $\mathcal{R}_i^{\Delta}(\phi_{\mathrm{E}})$ is similarly defined in terms of $\left\{\mathcal{C}_i^{\Delta}(\phi_{\mathrm{E}}, \phi'_{\mathrm{E}})\right\}_{\phi'_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}}$ as (3.35) as

$$\mathcal{R}_i^{\Delta}(\phi_{\mathrm{E}}) \triangleq \left\{ \bigcap_{\phi'_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}, \phi'_{\mathrm{E}} \neq \phi_{\mathrm{E}}} \mathcal{C}_i^{\Delta}(\phi_{\mathrm{E}}, \phi'_{\mathrm{E}}) \right\} \cap \mathcal{R}_i.$$

Given $\phi_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}$, the extended PBPO algorithm searches a person-by-person optimal remote strategy candidate $\phi_i^{\Delta}(\phi_{\mathrm{E}})$ which achieves an operation point in the person-by-person privacy concern region $\mathcal{R}_i^{\Delta}(\phi_{\mathrm{E}})$ as:

1. A person-by-person optimal remote strategy candidate $\phi_i^{\Delta}(\phi_{\mathrm{E}})$ of intercepted DM_i is the following deterministic likelihood-based test

$$\begin{aligned}
&\phi_i^{\Delta}(\phi_{\mathrm{E}}) \\
&= \arg\min_{\phi_i \in \Phi_i} \eta r_{\mathrm{F}}(\phi_1, \ldots, \phi_i, \ldots, \phi_n, \phi_{\mathrm{F}}) - (1-\eta) r_{\mathrm{E}}(\phi_1, \ldots, \phi_i, \ldots, \phi_k, \phi_{\mathrm{E}}),
\end{aligned} \tag{3.39}$$

   if it achieves an operation point on the boundary $\partial\mathcal{R}_i^{\Delta}(\phi_{\mathrm{E}}) \cap \partial\mathcal{R}_i$;

2. Otherwise, search a person-by-person optimal candidate $\phi_i^{\Delta}(\phi_{\mathrm{E}})$ of intercepted DM_i through deterministic likelihood-based tests which achieve operation points in the set $\bigcup_{\phi'_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}, \phi'_{\mathrm{E}} \neq \phi_{\mathrm{E}}} \{\partial \mathcal{R}_i^{\Delta}(\phi_{\mathrm{E}}) \cap \partial \mathcal{R}_i \cap \partial \mathcal{C}_i^{\Delta}(\phi_{\mathrm{E}}, \phi'_{\mathrm{E}})\}$ and randomized strategies of two deterministic likelihood-based tests which achieve operation points in the following set

$$\bigcup_{\substack{\phi'_{\mathrm{E}},\, \phi''_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}} \\ \phi'_{\mathrm{E}} \neq \phi_{\mathrm{E}},\, \phi''_{\mathrm{E}} \neq \phi_{\mathrm{E}},\, \phi'_{\mathrm{E}} \neq \phi''_{\mathrm{E}}}} \left\{\partial \mathcal{R}_i^{\Delta}(\phi_{\mathrm{E}}) \cap \partial \mathcal{C}_i^{\Delta}(\phi_{\mathrm{E}}, \phi'_{\mathrm{E}}) \cap \partial \mathcal{C}_i^{\Delta}(\phi_{\mathrm{E}}, \phi''_{\mathrm{E}})\right\}. \quad (3.40)$$

Algorithm 3.2 in the appendix of this chapter is the extended PBPO algorithm to design an optimal privacy-concerned distributed Bayesian hypothesis testing network.

3.4 Equivalent Privacy-Preserving Bayesian Testing Problems

Two privacy-preserving distributed Bayesian hypothesis testing problems have been discussed. They address both the objectives of improving the hypothesis testing performance and suppressing the privacy leakage in different ways. In the following theorems, the two problems are shown to be equivalent, i.e., there always exist a privacy-constrained problem and a privacy-concerned problem which lead to the same optimal privacy-preserving distributed hypothesis testing design.

Theorem 3.7. *Given $0 < \eta \leq 1$, consider a privacy-concerned Bayesian hypothesis testing problem:*

$$\begin{aligned}&(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)\\ =& \underset{(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) \in \Phi_1 \times \cdots \times \Phi_n \times \Phi_{\mathrm{F}}}{\arg\min} \eta r_{\mathrm{F}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) - (1-\eta) r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k).\end{aligned}$$

Let $\lambda = r_{\mathrm{E}}^{\min}(\phi_1^*, \ldots, \phi_k^*)$. Then, $(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)$ is also an optimal design for the following privacy-constrained Bayesian hypothesis testing problem:

$$\begin{aligned}(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*) = \underset{(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) \in \Phi_1 \times \cdots \times \Phi_n \times \Phi_{\mathrm{F}}}{\arg\min} & \quad r_{\mathrm{F}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}})\\ \text{s.t.} & \quad r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k) \geq \lambda.\end{aligned}$$

Proof. For any distributed hypothesis testing network design $(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}})$, from the definition of an optimal privacy-concerned distributed hypothesis testing network design $(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)$, the following inequality always holds as

$$\begin{aligned}&\eta r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*) - (1-\eta) r_{\mathrm{E}}^{\min}(\phi_1^*, \ldots, \phi_k^*)\\ \leq\ &\eta r_{\mathrm{F}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) - (1-\eta) r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k).\end{aligned}$$

For any distributed hypothesis testing network design $(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}})$ which satisfies the privacy leakage suppression constraint, the following inequality always holds as

$$r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k) \geq \lambda = r_{\mathrm{E}}^{\min}(\phi_1^*, \ldots, \phi_k^*).$$

Then, for any distributed hypothesis testing network design $(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}})$ which satisfies the privacy leakage suppression constraint, the above inequalities lead to

$$\begin{aligned} &\eta r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*) - (1-\eta) r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k) \\ \leq\ &\eta r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*) - (1-\eta) r_{\mathrm{E}}^{\min}(\phi_1^*, \ldots, \phi_k^*) \\ \leq\ &\eta r_{\mathrm{F}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) - (1-\eta) r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k), \end{aligned}$$

i.e.,

$$r_{\mathrm{F}}(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*) \leq r_{\mathrm{F}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}).$$

Further, the optimal privacy-concerned distributed hypothesis testing network design $(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)$ satisfies the privacy leakage suppression constraint. Therefore, $(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)$ is an optimal hypothesis testing network design for the equivalent privacy-constrained distributed Bayesian hypothesis testing problem. □

Theorem 3.8. *Given $\lambda \leq \gamma$, consider a privacy-constrained Bayesian hypothesis testing problem:*

$$\begin{aligned} (\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*) = \underset{(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) \in \Phi_1 \times \cdots \times \Phi_n \times \Phi_{\mathrm{F}}}{\arg\min} \quad & r_{\mathrm{F}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) \\ \text{s.t.} \quad & r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k) \geq \lambda. \end{aligned}$$

Denote the non-negative optimal dual Lagrange variable for the privacy leakage suppression constraint $r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k) \geq \lambda$ by α^* and let $\eta = \begin{cases} 1 & , \text{ if } \alpha^* = 0 \\ \dfrac{1}{1+\alpha^*}, & \text{if } \alpha^* > 0 \end{cases}$. Then, $(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)$ is also an optimal design for the following privacy-concerned Bayesian hypothesis testing problem:

$$\begin{aligned} &(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*) \\ = &\underset{(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) \in \Phi_1 \times \cdots \times \Phi_n \times \Phi_{\mathrm{F}}}{\arg\min} \quad \eta r_{\mathrm{F}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) - (1-\eta) r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k). \end{aligned}$$

Proof. Let $L(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}, \alpha) = r_{\mathrm{F}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) - \alpha(r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k) - \lambda)$ with a non-negative Lagrange multiplier $\alpha \geq 0$ denote a Lagrangian for the privacy-constrained problem and let $(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*, \alpha^*)$ be an optimum. Since the Karush-Kuhn-Tucker (KKT) conditions are necessary for the optimum, the optimal solution has to satisfy the complementary slackness condition

$$\alpha^*(r_{\mathrm{E}}^{\min}(\phi_1^*, \ldots, \phi_k^*) - \lambda) = 0.$$

If $\alpha^* = 0$, $(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)$ is an optimal design of the following privacy-concerned problem:

$$\begin{aligned}
&(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*) \\
=& \underset{(\phi_1,\ldots,\phi_n,\phi_{\mathrm{F}})\in\Phi_1\times\cdots\times\Phi_n\times\Phi_{\mathrm{F}}}{\arg\min} r_{\mathrm{F}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) - 0 \cdot (r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k) - \lambda) \\
=& \underset{(\phi_1,\ldots,\phi_n,\phi_{\mathrm{F}})\in\Phi_1\times\cdots\times\Phi_n\times\Phi_{\mathrm{F}}}{\arg\min} r_{\mathrm{F}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) - (1-1) r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k).
\end{aligned}$$

If $\alpha^* > 0$, $r_{\mathrm{E}}^{\min}(\phi_1^*, \ldots, \phi_k^*) = \lambda$ based on the complementary slackness condition. Then, let $\eta = \frac{1}{1+\alpha^*}$. It follows that $(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*)$ is an optimal design of the following privacy-concerned problem:

$$\begin{aligned}
&(\phi_1^*, \ldots, \phi_n^*, \phi_{\mathrm{F}}^*) \\
=& \underset{(\phi_1,\ldots,\phi_n,\phi_{\mathrm{F}})\in\Phi_1\times\cdots\times\Phi_n\times\Phi_{\mathrm{F}}}{\arg\min} r_{\mathrm{F}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) - \alpha^* (r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k) - \lambda) \\
=& \underset{(\phi_1,\ldots,\phi_n,\phi_{\mathrm{F}})\in\Phi_1\times\cdots\times\Phi_n\times\Phi_{\mathrm{F}}}{\arg\min} \eta r_{\mathrm{F}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) - (1-\eta)(r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k) - \lambda) \\
=& \underset{(\phi_1,\ldots,\phi_n,\phi_{\mathrm{F}})\in\Phi_1\times\cdots\times\Phi_n\times\Phi_{\mathrm{F}}}{\arg\min} \eta r_{\mathrm{F}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) - (1-\eta) r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k).
\end{aligned}$$

□

Equivalent privacy-preserving distributed Bayesian hypothesis testing problems address the objectives of suppressing privacy leakage and improving hypothesis testing performance from different perspectives. Theorems 3.7 and 3.8 show that an optimal privacy-preserving distributed Bayesian hypothesis testing network design can be interpreted in both the privacy-constrained and privacy-concerned optimality senses.

3.5 Numerical Examples

In this section, optimal privacy-preserving distributed Bayesian hypothesis testing network designs of a simple parallel model are obtained by using the proposed extended PBPO algorithms; their hypothesis testing performances and privacy leakages are shown and compared; and interesting observations are analyzed.

Consider the system model in Figure 3.1 with a binary hypothesis H, i.e., $s = 2$, two remote decision makers, i.e., $n = 2$, and binary decisions M_1, M_2, H_{F}, H_{E}, i.e., $s = s_1 = s_2 = 2$. Conditionally independent remote observations are generated following normal distributions as $Y_1|H = 0, Y_2|H = 0 \sim \mathcal{N}(0, 1)$ and $Y_1|H = 1, Y_2|H = 1 \sim \mathcal{N}(1, 1)$. The non-negative decision costs of the FC are assigned as $c_{\mathrm{F}}(0, 0) = c_{\mathrm{F}}(1, 1) = 0$ and $c_{\mathrm{F}}(0, 1) = c_{\mathrm{F}}(1, 0) = 1$. Thus, the Bayesian risk $r_{\mathrm{F}}(\phi_1, \phi_2, \phi_{\mathrm{F}})$ reduces to the error probability of fusion decision given a hypothesis testing network design $(\phi_1, \phi_2, \phi_{\mathrm{F}})$.

Powerful EVE

Here, consider the case that both DM-FC links are open-access and assume a powerful EVE who intercepts all remote decisions, i.e., $k = n = 2$. Two decision cost assignments of the EVE are considered. The first case assumes that the EVE concerns more about its miss probability $p_{H_{\mathrm{E}}|H}(0|1)$ and assigns the non-negative decision costs of the EVE as $c_{\mathrm{E}}(0,0) = c_{\mathrm{E}}(1,1) = 0$, $c_{\mathrm{E}}(0,1) = 2$, and $c_{\mathrm{E}}(1,0) = 1$. In the second case, the EVE is assumed to have the same decision cost assignment as the FC such that $c_{\mathrm{E}}(0,0) = c_{\mathrm{E}}(1,1) = 0$ and $c_{\mathrm{E}}(0,1) = c_{\mathrm{E}}(1,0) = 1$. Next, set the prior probability as $p_H(0) = p_H(1) = 0.5$.

Figures 3.4 and 3.5 compare the optimal privacy-constrained designs and optimal privacy-concerned designs, respectively. The numerical results show the trade-off of the hypothesis testing performance and privacy leakage risk. In Figure 3.4, the privacy-preserving performance is strengthened, i.e., increasing $r_{\mathrm{E}}^{\min}(\phi_1^*, \phi_2^*)$, at the cost of a worse hypothesis testing performance, i.e., increasing $r_{\mathrm{F}}(\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}^*)$. In Figure 3.5, the hypothesis testing performance is improved, i.e., decreasing $r_{\mathrm{F}}(\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}^*)$, at the cost of a weaker privacy-preserving performance, i.e., decreasing $r_{\mathrm{E}}^{\min}(\phi_1^*, \phi_2^*)$. For each decision cost assignment of the EVE, setting $\lambda = 0$ in the privacy-constrained problem or $\eta = 1$ in the privacy-concerned problem will lead to an optimal design for the distributed Bayesian hypothesis testing problem without considering suppression of privacy leakage. In Figure 3.4, an optimal privacy-constrained design is an optimal design without considering privacy leakage suppression when λ is smaller than a certain threshold. That is because the Bayesian privacy leakage measure of an optimal distributed hypothesis testing design without considering privacy leakage suppression already satisfies the privacy leakage suppression constraint when the desired lower bound λ is small. If the EVE and the FC have the same decision cost assignment, the two measures $r_{\mathrm{F}}(\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}^*)$ and $r_{\mathrm{E}}^{\min}(\phi_1^*, \phi_2^*)$ of an optimal privacy-constrained or optimal privacy-concerned design are always equal, i.e., the red square line fully overlaps the pink circle line in Figures 3.4 and 3.5. That is because the FC and the EVE have the same observations, decision cost assignment, and therefore minimize the same Bayesian risk function. This property also explains the observation in Figure 3.5 that an optimal privacy-concerned distributed Bayesian hypothesis testing design always has $r_{\mathrm{F}}(\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}^*) = r_{\mathrm{E}}^{\min}(\phi_1^*, \phi_2^*) = \max_{(\phi_1,\phi_2)\in\Phi_1\times\Phi_2} r_{\mathrm{E}}^{\min}(\phi_1, \phi_2)$ when $\eta < 0.5$ and $r_{\mathrm{F}}(\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}^*) = r_{\mathrm{E}}^{\min}(\phi_1^*, \phi_2^*) = \min_{(\phi_1,\phi_2,\phi_{\mathrm{F}})\in\Phi_1\times\Phi_2\times\Phi_{\mathrm{F}}} r_{\mathrm{F}}(\phi_1, \phi_2, \phi_{\mathrm{F}})$ when $\eta > 0.5$ if the EVE and the FC have the same decision cost assignment.

Single intercepted remote decision

Here, the EVE is assumed to intercept the DM_1-FC link and to have the same decision cost assignment as the FC. It is to verify if a useless remote decision M_1 for the EVE can improve the hypothesis testing performance of the FC. The maximum privacy leakage suppression guarantee is set for an optimal privacy-constrained distributed Bayesian hypothesis testing design, i.e., $\lambda = \gamma$. The privacy leakage

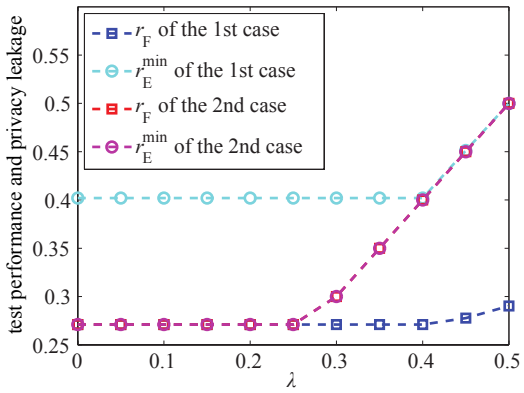


Figure 3.4: The hypothesis testing performances r_{F} and privacy leakage risks $r_{\mathrm{E}}^{\min}$ of optimal privacy-constrained distributed Bayesian hypothesis testing designs against different privacy leakage suppression guarantees λ and decision cost assignments of the EVE. Here, the EVE is powerful to intercept all remote decisions. The prior probability is set as $p_H(0) = p_H(1) = 0.5$. If the EVE and the FC have the same decision cost assignment, $r_{\mathrm{F}}(\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}^*) = r_{\mathrm{E}}^{\min}(\phi_1^*, \phi_2^*)$.

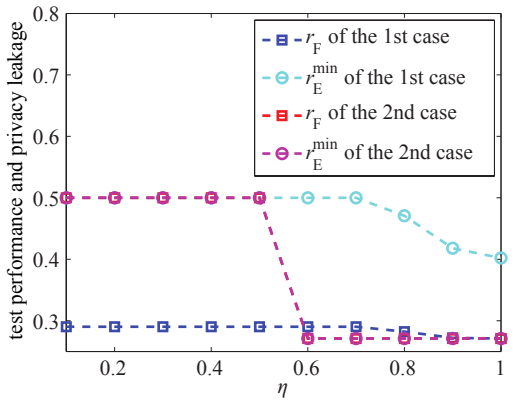


Figure 3.5: The hypothesis testing performances r_{F} and privacy leakage risks $r_{\mathrm{E}}^{\min}$ of optimal privacy-concerned distributed Bayesian hypothesis testing designs against different concern weights η and decision cost assignments of the EVE. Here, the EVE is powerful to intercept all remote decisions. The prior probability is set as $p_H(0) = p_H(1) = 0.5$. If the EVE and the FC have the same decision cost assignment, $r_{\mathrm{F}}(\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}^*) = r_{\mathrm{E}}^{\min}(\phi_1^*, \phi_2^*)$.

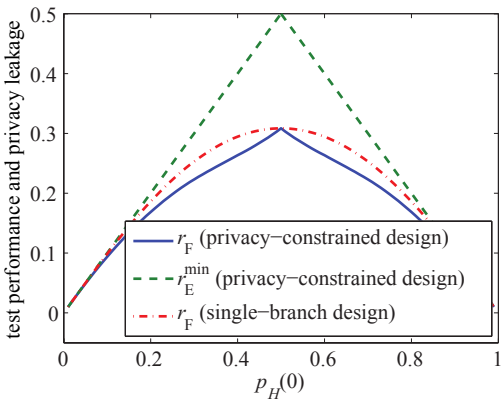


Figure 3.6: The hypothesis testing performances r_{F} and privacy leakage risks $r_{\mathrm{E}}^{\min}$ of optimal privacy-constrained distributed Bayesian hypothesis testing designs against different prior probabilities $p_H(0)$. Here, the EVE is assumed to intercept M_1 and has the same decision cost assignment as the FC. The maximum privacy leakage suppression guarantee is set as $\lambda = \gamma$. The hypothesis testing performances of optimal single-branch designs, which also realize the maximum privacy leakage suppression guarantee, are shown as benchmarks.

suppression constraint requires $r_{\mathrm{E}}^{\min}(\phi_1^*) \geq \lambda = \gamma$ while $r_{\mathrm{E}}^{\min}(\phi_1^*) \leq \gamma$. An optimal privacy-constrained distributed Bayesian hypothesis testing design will always have $r_{\mathrm{E}}^{\min}(\phi_1^*) = \gamma$. Note that the maximum privacy leakage suppression guarantee can also be realized through cutting off DM_1-FC link and forcing the EVE to infer the hypothesis by the knowledge of the prior probability only.

Figure 3.6 shows the hypothesis testing performance and privacy leakage risk of an optimal privacy-constrained distributed Bayesian hypothesis testing design. As a benchmark, the hypothesis testing performance of an optimal single-branch design, which cuts off the intercepted DM_1-FC link and optimizes the other protected link to minimize the Bayesian risk of fusion decision, is also shown. Comparing the hypothesis testing performances of an optimal privacy-constrained design and an optimal single-branch design, it can be concluded that the intercepted remote decision maker can be optimally designed to transmit data which is useless for the EVE but is useful to make the fusion decision jointly with the information from the other optimally designed remote decision maker.

3.6 Summary

In this chapter, privacy-preserving distributed Bayesian hypothesis testing problems are formulated and studied. In contrast to optimal distributed Bayesian hypothesis testing network designs, the optimality of deterministic likelihood-based test (or

LRT) does not always hold for the remote strategies of intercepted remote decision makers in an optimal privacy-preserving design. The standard PBPO algorithm is extended to design an optimal privacy-preserving distributed Bayesian hypothesis testing network based on the obtained optimality characteristics.

3.7 Appendix

Algorithm 3.1 The extended PBPO algorithm to design an optimal privacy-constrained distributed Bayesian hypothesis testing network.

generate a sufficiently large number sets of initial remote strategies $(\phi_1, \ldots, \phi_n)$ which satisfy the privacy leakage suppression constraint.
given a set of initial remote strategies
while $r_{\mathrm{F}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}})$ does not satisfy the convergence criterion **do**
  $\phi_{\mathrm{F}} \leftarrow \phi_{\mathrm{F}}^{\Delta}$ in (3.27).
  for $i \in \{1, \ldots, n\}$ **do**
    $\phi_i \leftarrow \phi_i^{\Delta}$ in (3.28).
    if $1 \leq i \leq k$ and $r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k) < \lambda$ **then**
      $\phi_i \leftarrow$
      use linear programming to find a person-by-person optimal remote strategy ϕ_i^{Δ} which achieves an operation point in the following person-by-person privacy constraint hyperplane intersection set $\bigcup_{\phi_{\mathrm{E}}, \phi'_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}, \phi_{\mathrm{E}} \neq \phi'_{\mathrm{E}}} \left\{ \partial \mathcal{R}_i^{\mathrm{P}\Delta} \cap \partial \mathcal{P}_i^{\Delta}(\phi_{\mathrm{E}}) \cap \partial \mathcal{P}_i^{\Delta}(\phi'_{\mathrm{E}}) \right\}$.
      if $\phi_i = null$ **then**
        $\phi_i \leftarrow$
        search a person-by-person optimal remote strategy ϕ_i^{Δ} which achieves an operation point in the set $\bigcup_{\phi_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}} \left\{ \partial \mathcal{R}_i^{\mathrm{P}\Delta} \cap \partial \mathcal{R}_i \cap \partial \mathcal{P}_i^{\Delta}(\phi_{\mathrm{E}}) \right\}$.
      end if
    end if
  end for
end while
compare obtained distributed hypothesis testing network designs corresponding to all sets of initial remote strategies.

output: the obtained distributed hypothesis testing network design which achieves the best hypothesis testing performance

Algorithm 3.2 The extended PBPO algorithm to design an optimal privacy-concerned distributed Bayesian hypothesis testing network.

generate a sufficiently large number sets of initial remote strategies $(\phi_1, \ldots, \phi_n)$.
given a set of initial remote strategies
while $\eta r_{\mathrm{F}}(\phi_1, \ldots, \phi_n, \phi_{\mathrm{F}}) - (1-\eta) r_{\mathrm{E}}^{\min}(\phi_1, \ldots, \phi_k)$ does not satisfy the convergence criterion **do**
  $\phi_{\mathrm{F}} \leftarrow \phi_{\mathrm{F}}^{\Delta}$ in (3.27).
  for $i \in \{k+1, \ldots, n\}$ **do**
    $\phi_i \leftarrow \phi_i^{\Delta}$ in (3.28).
  end for
  for $i \in \{1, \ldots, k\}$ **do**
    for $\phi_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}$ **do**
      $\phi_i^{\Delta}(\phi_{\mathrm{E}}) \leftarrow$ (3.39).
      if $\boldsymbol{p}_i(\phi_i^{\Delta}(\phi_{\mathrm{E}})) \notin \{\partial\mathcal{R}_i^{\Delta}(\phi_{\mathrm{E}}) \cap \partial\mathcal{R}_i\}$ **then**
        $\phi_i^{\Delta}(\phi_{\mathrm{E}}) \leftarrow$
        use linear programming to find a person-by-person optimal candidate $\phi_i^{\Delta}(\phi_{\mathrm{E}})$ which achieves an operation point in the set (3.40).
        if $\phi_i^{\Delta}(\phi_{\mathrm{E}}) = null$ **then**
          $\phi_i^{\Delta}(\phi_{\mathrm{E}}) \leftarrow$
          search a person-by-person optimal candidate $\phi_i^{\Delta}(\phi_{\mathrm{E}})$ which achieves an operation point in the set $\bigcup_{\phi'_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}, \phi'_{\mathrm{E}} \neq \phi_{\mathrm{E}}} \{\partial\mathcal{R}_i^{\Delta}(\phi_{\mathrm{E}}) \cap \partial\mathcal{R}_i \cap \partial\mathcal{C}_i^{\Delta}(\phi_{\mathrm{E}}, \phi'_{\mathrm{E}})\}$.
        end if
      end if
    end for
    $\phi_i \leftarrow$ the optimal remote strategy in the candidate set $\{\phi_i^{\Delta}(\phi_{\mathrm{E}})\}_{\phi_{\mathrm{E}} \in \Phi_{\mathrm{E}}^{\mathrm{D}}}$ which minimizes $\eta r_{\mathrm{F}}(\phi_1, \ldots, \phi_i^{\Delta}(\phi_{\mathrm{E}}), \ldots, \phi_n, \phi_{\mathrm{F}}) - (1-\eta) r_{\mathrm{E}}(\phi_1, \ldots, \phi_i^{\Delta}(\phi_{\mathrm{E}}), \ldots, \phi_k, \phi_{\mathrm{E}})$.
  end for
end while
compare obtained distributed hypothesis testing network designs corresponding to all sets of initial remote strategies.

output: the obtained distributed hypothesis testing network design which achieves the minimal weighted sum objective

Chapter 4

Privacy-Preserving Distributed Neyman-Pearson Hypothesis Test

In Chapter 3, an optimal privacy-preserving distributed hypothesis testing network is designed based on operational Bayesian hypothesis testing performance and privacy leakage measures. However, the discussed privacy-preserving distributed Bayesian hypothesis testing problems cannot be formulated if the information of the hypothesis prior distribution and the decision cost assignment is not available. In this chapter, a privacy-preserving distributed Neyman-Pearson hypothesis testing problem is formulated by using operational Neyman-Pearson hypothesis testing performance and privacy leakage measures; and optimal privacy-preserving distributed Neyman-Pearson hypothesis testing design is characterized.

4.1 Distributed Hypothesis Test in the Presence of an Eavesdropper

System model

The studied parallel model in Figure 4.1 consists of a binary hypothesis H, two remote decision makers $\{\mathrm{DM}_i\}_{i=1}^2$, an FC, and an EVE. The hypothesis H is defined on the alphabet $\mathcal{H} = \{0, 1\}$. Each remote decision maker DM_i independently makes a binary remote decision M_i defined on the alphabet $\mathcal{M} = \{0, 1\}$ based on the continuous random observation Y_i defined on the alphabet $\mathcal{Y}_i$. The likelihoods of the remote observation Y_i are denoted by p.d.f.s $\{f_{Y_i|H}(\cdot|h)\}_{h\in\mathcal{H}}$. The remote observations are assumed to be conditionally independent given any hypothesis $h \in \mathcal{H}$, i.e.,

$$f_{Y_1,Y_2|H}(y_1, y_2|h) = f_{Y_1|H}(y_1|h) f_{Y_2|H}(y_2|h). \tag{4.1}$$

The remote decisions are transmitted to the FC through error-free two-bit-rate links. Based on the remote decisions (M_1, M_2), the FC makes a binary fusion decision H_{F} to infer the hypothesis H. The EVE is assumed to intercept the first

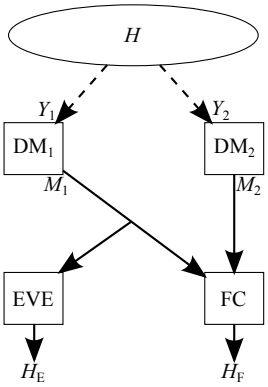


Figure 4.1: A parallel distributed hypothesis testing network in the presence of an EVE. The first remote decision M_1 is intercepted by the EVE.

remote decision M_1 and makes a binary eavesdropper decision $H_{\rm E}$ to infer the hypothesis H as well. Here, independent, possibly randomized, decision strategies [57] of the $\{{\rm DM}_i\}_{i=1}^2$, the FC, and the EVE are denoted by $\{\phi_i\}_{i=1}^2$, $\phi_{\rm F}$, and $\phi_{\rm E}$, respectively:

$$\begin{aligned} \phi_i &: \mathcal{Y}_i \to \mathcal{M},\ i = 1,\ 2, \\ \phi_{\rm F} &: \mathcal{M} \times \mathcal{M} \to \mathcal{H}, \\ \phi_{\rm E} &: \mathcal{M} \to \mathcal{H}. \end{aligned} \tag{4.2}$$

Note that the (randomized) strategies can be equivalently represented by conditional p.m.f.s $\{p_{M_i|Y_i}\}_{i=1}^2$, $p_{H_{\rm F}|M^2}$, and $p_{H_{\rm E}|M_1}$. Let Φ_i, $\Phi_{\rm F}$, and $\Phi_{\rm E}$ denote the (randomized) decision strategy sets of the ${\rm DM}_i$, the FC, and the EVE, i.e., $\phi_i \in \Phi_i$, $\phi_{\rm F} \in \Phi_{\rm F}$, and $\phi_{\rm E} \in \Phi_{\rm E}$.

Neyman-Pearson privacy leakage measure

Similar as the settings in the previous chapter, the EVE is assumed to be informed about all needed statistics of the distributed hypothesis testing network. That means the worst privacy leakage scenario is considered since the statistical knowledge enables the EVE to always choose the best strategy to infer the correct hypothesis. The choices of the privacy leakage model and measure follow from the privacy-preserving objective of the system designer. In this chapter, the privacy leakage is modeled as a Neyman-Pearson hypothesis test made by the informed EVE based on the intercepted remote decision M_1. Given a distributed hypothesis testing network design $(\phi_1, \phi_2, \phi_{\rm F})$, the privacy leakage is measured by the minimal miss probability of eavesdropper decision subject to an upper bound constraint on the false-alarm probability of eavesdropper decision:

$$p_{\rm EM}^{\min}(\phi_1) = \min_{\phi_{\rm E} \in \Phi_{\rm E}} p_{\rm EM}(\phi_1, \phi_{\rm E}),\ \text{s.t. } p_{\rm EF}(\phi_1, \phi_{\rm E}) \le \lambda_{\rm E}, \tag{4.3}$$

where the upper bound satisfies $0 \leq \lambda_{\mathrm{E}} \leq 1$; the miss probability and false-alarm probability are in terms of the remote strategy ϕ_1 and eavesdropper strategy ϕ_{E} as

$$\begin{aligned} p_{\mathrm{EM}}(\phi_1, \phi_{\mathrm{E}}) &= p_{H_{\mathrm{E}}|H}(0|1) = \int_{\mathcal{Y}_1} \sum_{m_1 \in \mathcal{M}} p_{H_{\mathrm{E}}|M_1}(0|m_1) p_{M_1|Y_1}(m_1|y_1) f_{Y_1|H}(y_1|1) dy_1, \\ p_{\mathrm{EF}}(\phi_1, \phi_{\mathrm{E}}) &= p_{H_{\mathrm{E}}|H}(1|0) = \int_{\mathcal{Y}_1} \sum_{m_1 \in \mathcal{M}} p_{H_{\mathrm{E}}|M_1}(1|m_1) p_{M_1|Y_1}(m_1|y_1) f_{Y_1|H}(y_1|0) dy_1. \end{aligned} \tag{4.4}$$

Given ϕ_1, the EVE makes a centralized Neyman-Pearson hypothesis test based on the discrete random observation M_1. Following from Property 2.2, an optimal eavesdropper strategy can be a deterministic LRT or a randomized strategy of two deterministic LRTs; the upper bound on the false-alarm probability of eavesdropper decision can always be achieved by an optimal eavesdropper strategy, i.e., the Neyman-Pearson privacy leakage measure can be equivalently rewritten as

$$p_{\mathrm{EM}}^{\min}(\phi_1) = \min_{\phi_{\mathrm{E}} \in \Phi_{\mathrm{E}}} p_{\mathrm{EM}}(\phi_1, \phi_{\mathrm{E}}), \text{ s.t. } p_{\mathrm{EF}}(\phi_1, \phi_{\mathrm{E}}) = \lambda_{\mathrm{E}}. \tag{4.5}$$

Remark 4.1. *Given an upper bound λ_{E} on the false-alarm probability of eavesdropper decision, there is a simple upper bound on the privacy leakage measure: For all $\phi_1 \in \Phi_1$,*

$$p_{\mathrm{EM}}^{\min}(\phi_1) \leq 1 - \lambda_{\mathrm{E}}. \tag{4.6}$$

Proof. Given an upper bound λ_{E} and a remote strategy $\phi_1 \in \Phi_1$, an optimal eavesdropper strategy achieves the operation point on the ROC curve and the upper bound λ_{E} on the false-alarm probability of eavesdropper decision. From Property 2.2, the ROC curve is always above the line $p_{\mathrm{ED}} = p_{\mathrm{EF}}$. It means that an optimal eavesdropper strategy achieves a detection probability of eavesdropper decision greater than or equal to the value λ_{E}, i.e., an optimal eavesdropper strategy achieves a miss probability of eavesdropper decision smaller than or equal to the value $1 - \lambda_{\mathrm{E}}$. □

Neyman-Pearson hypothesis testing performance measure

Give a distributed hypothesis testing network design $(\phi_1, \phi_2, \phi_{\mathrm{F}})$. If the corresponding false-alarm probability of fusion decision satisfies an upper bound constraint $p_{\mathrm{FF}}(\phi_1, \phi_2, \phi_{\mathrm{F}}) \leq \lambda_{\mathrm{F}}$ where $0 \leq \lambda_{\mathrm{F}} \leq 1$ and

$$\begin{aligned} & p_{\mathrm{FF}}(\phi_1, \phi_2, \phi_{\mathrm{F}}) = p_{H_{\mathrm{F}}|H}(1|0) \\ = & \int_{\mathcal{Y}_1 \times \mathcal{Y}_2} \sum_{(m_1, m_2) \in \mathcal{M} \times \mathcal{M}} p_{H_{\mathrm{F}}|M_1, M_2}(1|m_1, m_2) \prod_{i=1}^{2} p_{M_i|Y_i}(m_i|y_i) f_{Y_i|H}(y_i|0) dy_1 dy_2, \end{aligned} \tag{4.7}$$

the hypothesis testing performance of the distributed hypothesis testing network design is measured by the miss probability of fusion decision as

$$\begin{aligned} & p_{\mathrm{FM}}(\phi_1, \phi_2, \phi_{\mathrm{F}}) = p_{H_{\mathrm{F}}|H}(0|1) \\ &= \int_{\mathcal{Y}_1 \times \mathcal{Y}_2} \sum_{(m_1, m_2) \in \mathcal{M} \times \mathcal{M}} p_{H_{\mathrm{F}}|M_1, M_2}(0|m_1, m_2) \prod_{i=1}^{2} p_{M_i|Y_i}(m_i|y_i) f_{Y_i|H}(y_i|1) dy_1 dy_2. \end{aligned} \tag{4.8}$$

4.2 Privacy-Constrained Distributed Neyman-Pearson Hypothesis Test

Problem formulation

Using the Neyman-Pearson hypothesis testing performance and privacy leakage measures, the privacy-constrained distributed Neyman-Pearson hypothesis testing problem is formulated as

$$\begin{aligned} (\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}^*) = \underset{(\phi_1, \phi_2, \phi_{\mathrm{F}}) \in \Phi_1 \times \Phi_2 \times \Phi_{\mathrm{F}}}{\arg\min} \quad & p_{\mathrm{FM}}(\phi_1, \phi_2, \phi_{\mathrm{F}}) \\ \text{s.t.} \quad & p_{\mathrm{FF}}(\phi_1, \phi_2, \phi_{\mathrm{F}}) \leq \lambda_{\mathrm{F}} \\ & p_{\mathrm{EM}}^{\min}(\phi_1) \geq \varphi, \end{aligned} \tag{4.9}$$

where φ is the privacy leakage suppression guarantee. Because of the privacy leakage upper bound in (4.6), the privacy-constrained optimization problem is feasible only if $\varphi \leq 1 - \lambda_{\mathrm{E}}$.

Characteristics of an optimal privacy-constrained design

For the distributed Neyman-Pearson hypothesis testing problem, the optimality of deterministic LRT does not always hold for an optimal fusion strategy but holds for optimal remote strategies. Here, the impact of the privacy leakage suppression constraint on the optimality of deterministic LRT is to be investigated. To this end, the person-by-person optimality argument is used.

Given an optimal privacy-constrained distributed hypothesis testing network design $(\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}^*)$, it follows from the person-by-person optimality argument that

$$\begin{aligned} \phi_{\mathrm{F}}^* = \underset{\phi_{\mathrm{F}} \in \Phi_{\mathrm{F}}}{\arg\min} \quad & p_{\mathrm{FM}}(\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}) \\ \text{s.t.} \quad & p_{\mathrm{FF}}(\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}) \leq \lambda_{\mathrm{F}} \\ & p_{\mathrm{EM}}^{\min}(\phi_1^*) \geq \varphi. \end{aligned} \tag{4.10}$$

Note that the privacy leakage suppression constraint does not depend on the fusion strategy ϕ_{F}. Therefore, the PBPO problem (4.10) reduces to

$$\begin{aligned} \phi_{\mathrm{F}}^* = \underset{\phi_{\mathrm{F}} \in \Phi_{\mathrm{F}}}{\arg\min}\ & p_{\mathrm{FM}}(\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}) \\ \text{s.t.}\quad & p_{\mathrm{FF}}(\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}) \le \lambda_{\mathrm{F}}, \end{aligned} \tag{4.11}$$

which can be seen as a centralized Neyman-Pearson hypothesis test with a discrete random observation sequence. From Property 2.2, an optimal fusion strategy ϕ_{F}^* of the privacy-constrained Neyman-Pearson hypothesis testing problem (4.9) can be a deterministic LRT or a randomized strategy of two deterministic LRTs. Further, an optimal privacy-constrained distributed hypothesis testing network $(\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}^*)$ always achieves the upper bound on the false-alarm probability of fusion decision, i.e., $p_{\mathrm{FF}}(\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}^*) = \lambda_{\mathrm{F}}$. That means the privacy-constrained distributed Neyman-Pearson hypothesis testing problem can be equivalently formulated as

$$\begin{aligned} (\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}^*) = \underset{(\phi_1, \phi_2, \phi_{\mathrm{F}}) \in \Phi_1 \times \Phi_2 \times \Phi_{\mathrm{F}}}{\arg\min}\ & p_{\mathrm{FM}}(\phi_1, \phi_2, \phi_{\mathrm{F}}) \\ \text{s.t.}\quad & p_{\mathrm{FF}}(\phi_1, \phi_2, \phi_{\mathrm{F}}) = \lambda_{\mathrm{F}} \\ & p_{\mathrm{EM}}^{\min}(\phi_1) \ge \varphi. \end{aligned} \tag{4.12}$$

The following discussion is based on (4.12) instead.

Theorem 4.1. *For the privacy-constrained Neyman-Pearson hypothesis testing problem (4.12), it is sufficient to consider a deterministic LRT for ϕ_2^*.*

Proof. Given an optimal privacy-constrained hypothesis testing network design $(\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}^*)$, it follows from the person-by-person optimality argument that

$$\begin{aligned} \phi_2^* = \underset{\phi_2 \in \Phi_2}{\arg\min}\ & p_{\mathrm{FM}}(\phi_1^*, \phi_2, \phi_{\mathrm{F}}^*) \\ \text{s.t.}\quad & p_{\mathrm{FF}}(\phi_1^*, \phi_2, \phi_{\mathrm{F}}^*) = \lambda_{\mathrm{F}} \\ & p_{\mathrm{EM}}^{\min}(\phi_1^*) \ge \varphi. \end{aligned} \tag{4.13}$$

The privacy leakage suppression constraint does not depend on the remote strategy ϕ_2. The PBPO problem is equivalent to

$$\begin{aligned} \phi_2^* = \underset{\phi_2 \in \Phi_2}{\arg\min}\ & p_{\mathrm{FM}}(\phi_1^*, \phi_2, \phi_{\mathrm{F}}^*) \\ \text{s.t.}\quad & p_{\mathrm{FF}}(\phi_1^*, \phi_2, \phi_{\mathrm{F}}^*) = \lambda_{\mathrm{F}}. \end{aligned} \tag{4.14}$$

Define

$$a_2^*(m_2, h_{\mathrm{F}}, h) \triangleq \int_{\mathcal{Y}_1} \sum_{m_1 \in \mathcal{M}} p_{H_{\mathrm{F}}|M_1,M_2}^*(h_{\mathrm{F}}|m_1, m_2) p_{M_1|Y_1}^*(m_1|y_1) f_{Y_1|H}(y_1|h) dy_1. \tag{4.15}$$

The miss probability and false-alarm probability of fusion decision in (4.14) can be expressed in terms of detection probability and false-alarm probability of remote decision M_2 respectively as

$$\begin{aligned} p_{\mathrm{FM}}(\phi_1^*,\phi_2,\phi_{\mathrm{F}}^*) &= \sum_{m_2\in\mathcal{M}} a_2^*(m_2,0,1)\int_{\mathcal{Y}_2} p_{M_2|Y_2}(m_2|y_2) f_{Y_2|H}(y_2|1)dy_2 \\ &= a_2^*(0,0,1)p_{M_2|H}(0|1) + a_2^*(1,0,1)p_{M_2|H}(1|1) \\ &= a_2^*(0,0,1) + (a_2^*(1,0,1) - a_2^*(0,0,1))p_{2\mathrm{D}}(\phi_2), \\ p_{\mathrm{FF}}(\phi_1^*,\phi_2,\phi_{\mathrm{F}}^*) &= \sum_{m_2\in\mathcal{M}} a_2^*(m_2,1,0)\int_{\mathcal{Y}_2} p_{M_2|Y_2}(m_2|y_2) f_{Y_2|H}(y_2|0)dy_2 \\ &= a_2^*(0,1,0)p_{M_2|H}(0|0) + a_2^*(1,1,0)p_{M_2|H}(1|0) \\ &= a_2^*(0,1,0) + (a_2^*(1,1,0) - a_2^*(0,1,0))p_{2\mathrm{F}}(\phi_2). \end{aligned} \tag{4.16}$$

Obviously, depending on the sign of the coefficient $a_2^*(1,0,1)-a_2^*(0,0,1)$, an optimal remote strategy ϕ_2^* of (4.14) maximizes or minimizes the detection probability of remote decision M_2 subject to that the corresponding false-alarm probability $p_{2\mathrm{F}}(\phi_2^*)$ satisfies $a_2^*(0,1,0) + (a_2^*(1,1,0) - a_2^*(0,1,0))p_{2\mathrm{F}}(\phi_2^*) = \lambda_{\mathrm{F}}$, i.e., the operation point $\boldsymbol{p}_2(\phi_2^*) = (p_{2\mathrm{F}}(\phi_2^*), p_{2\mathrm{D}}(\phi_2^*))$ is on the upper or lower boundary of the operation region $\mathcal{R}_2$. From Property 2.1, an optimal remote strategy ϕ_2^* is a deterministic LRT and can be specified as:

$$\text{If } a_2^*(1,0,1) - a_2^*(0,0,1) \le 0,\ M_2 = \phi_2^*(y_2) = \begin{cases} 0, & \text{if } \dfrac{f_{Y_2|H}(y_2|0)}{f_{Y_2|H}(y_2|1)} \ge \dfrac{1}{\rho_2} \\ 1, & \text{otherwise} \end{cases}, \tag{4.17}$$

where the non-negative test threshold ρ_2 and the corresponding set $\mathcal{A}_2(\rho_2) = \left\{ y_2 \,\middle|\, \frac{f_{Y_2|H}(y_2|0)}{f_{Y_2|H}(y_2|1)} \ge \frac{1}{\rho_2} \right\}$ satisfy

$$\int_{\mathcal{A}_2^c(\rho_2)} f_{Y_2|H}\left(y_2|0\right) dy_2 = \frac{\lambda_{\mathrm{F}} - a_2^*(0,1,0)}{a_2^*(1,1,0) - a_2^*(0,1,0)};$$

or

$$\text{If } a_2^*(1,0,1) - a_2^*(0,0,1) > 0,\ M_2 = \phi_2^*(y_2) = \begin{cases} 0, & \text{if } \dfrac{f_{Y_2|H}(y_2|0)}{f_{Y_2|H}(y_2|1)} \le \dfrac{1}{\rho_2} \\ 1, & \text{otherwise} \end{cases}, \tag{4.18}$$

where the non-negative test threshold ρ_2 and the corresponding set $\mathcal{A}_2(\rho_2)$ satisfy

$$\int_{\mathcal{A}_2(\rho_2)} f_{Y_2|H}\left(y_2|0\right) dy_2 = \frac{\lambda_{\mathrm{F}} - a_2^*(0,1,0)}{a_2^*(1,1,0) - a_2^*(0,1,0)}.$$

□

Table 4.1: Eavesdropper operation points corresponding to the four deterministic eavesdropper strategies given $\phi_1 \in \Phi_1$.

eavesdropper strategy	operation point
$H_{\mathrm{E}} = \phi_{\mathrm{E}}(m_1) = 0$	$\boldsymbol{p}_{\mathrm{E}}(\phi_1, \phi_{\mathrm{E}}) = (0, 0)$
$H_{\mathrm{E}} = \phi_{\mathrm{E}}(m_1) = m_1$	$\boldsymbol{p}_{\mathrm{E}}(\phi_1, \phi_{\mathrm{E}}) = \boldsymbol{p}_1(\phi_1) = (p_{1\mathrm{F}}(\phi_1), p_{1\mathrm{D}}(\phi_1))$
$H_{\mathrm{E}} = \phi_{\mathrm{E}}(m_1) = 1$	$\boldsymbol{p}_{\mathrm{E}}(\phi_1, \phi_{\mathrm{E}}) = (1, 1)$
$H_{\mathrm{E}} = \phi_{\mathrm{E}}(m_1) = \lvert m_1 - 1 \rvert$	$\boldsymbol{p}_{\mathrm{E}}(\phi_1, \phi_{\mathrm{E}}) = (1 - p_{1\mathrm{F}}(\phi_1), 1 - p_{1\mathrm{D}}(\phi_1))$

In the following theorems, it will be shown that the optimality of deterministic LRT for the intercepted remote decision maker DM_1 depends on the false-alarm probability upper bounds λ_{F} and λ_{E}. The analysis is based on the person-by-person optimality argument and the operation region $\mathcal{R}_1$.

The privacy leakage suppression constraint takes effect in the following PBPO problem: Given an optimal privacy-constrained distributed network $(\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}^*)$,

$$\begin{aligned} \phi_1^* = \underset{\phi_1 \in \Phi_1}{\arg\min}\ & p_{\mathrm{FM}}(\phi_1, \phi_2^*, \phi_{\mathrm{F}}^*) \\ \text{s.t.}\quad & p_{\mathrm{FF}}(\phi_1, \phi_2^*, \phi_{\mathrm{F}}^*) = \lambda_{\mathrm{F}} \\ & p_{\mathrm{EM}}^{\min}(\phi_1) \geq \varphi. \end{aligned} \tag{4.19}$$

Define the privacy-constrained operation region of the intercepted DM_1 as

$$\mathcal{R}_1^{\mathrm{P}} \triangleq \mathcal{R}_1 \cap \left\{ \boldsymbol{p}_1(\phi_1) \,\middle|\, p_{\mathrm{EM}}^{\min}(\phi_1) \geq \varphi \right\}. \tag{4.20}$$

To characterize the privacy-constrained operation region $\mathcal{R}_1^{\mathrm{P}}$, how the operation region of the EVE relates with the remote strategy ϕ_1 is studied first.

Given $\phi_1 \in \Phi_1$, define the eavesdropper operation point achieved by an eavesdropper strategy ϕ_{E} as

$$\boldsymbol{p}_{\mathrm{E}}(\phi_1, \phi_{\mathrm{E}}) \triangleq (p_{\mathrm{EF}}(\phi_1, \phi_{\mathrm{E}}), p_{\mathrm{ED}}(\phi_1, \phi_{\mathrm{E}})); \tag{4.21}$$

and define the operation region of the EVE as

$$\mathcal{R}_{\mathrm{E}}(\phi_1) \triangleq \left\{ \boldsymbol{p}_{\mathrm{E}}(\phi_1, \phi_{\mathrm{E}}) \,\middle|\, \phi_{\mathrm{E}} \in \Phi_{\mathrm{E}} \right\}. \tag{4.22}$$

There are four deterministic eavesdropper strategies as listed in Table 4.1: Given an intercepted remote decision $m_1 \in \mathcal{M}$, the EVE can always make a decision 0 regardless of the intercepted remote decision; the EVE can accept the remote decision and make the same eavesdropper decision; the EVE can always make a decision 1 regardless of the intercepted remote decision; or the EVE can make the eavesdropper decision by flipping the remote decision. As shown in Figure 4.2, an operation region of the EVE $\mathcal{R}_{\mathrm{E}}(\phi_1)$ is a parallelogram confined by operation points achieved by the four deterministic eavesdropper strategies.

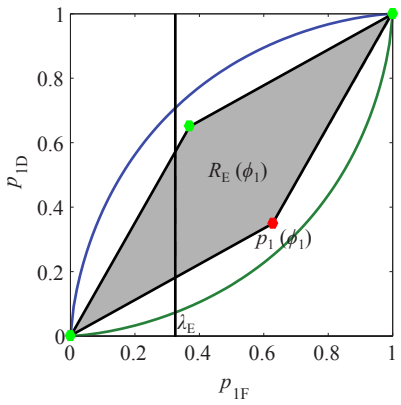


Figure 4.2: Illustration of an operation region of the EVE given $\phi_1 \in \Phi_1$. The hexagon points can be achieved by deterministic eavesdropper strategies. The red hexagon point coincides the operation point $\boldsymbol{p}_1(\phi_1)$ and can be achieved if the EVE simply makes the same decision as the intercepted remote decision m_1. All other operation points can be achieved by randomized eavesdropper strategies.

Given $\phi_1 \in \Phi_1$ which violates the privacy leakage suppression constraint of $p_{\mathrm{EM}}^{\min}(\phi_1) \geq \varphi$, an optimal eavesdropper strategy ϕ_{E}^* achieves the operation point $(\lambda_{\mathrm{E}}, p_{\mathrm{ED}}(\phi_1, \phi_{\mathrm{E}}^*))$ on the ROC of $\mathcal{R}_{\mathrm{E}}(\phi_1)$ with $p_{\mathrm{ED}}(\phi_1, \phi_{\mathrm{E}}^*) > 1 - \varphi$. Thus, the privacy leakage suppression constraint is violated if an operation point $\boldsymbol{p}_1(\phi_1)$ is above the lines through $(0,0)$, $(\lambda_{\mathrm{E}}, 1-\varphi)$, and through $(1,1)$, $(\lambda_{\mathrm{E}}, 1-\varphi)$, or below the lines through $(0,0)$, $(1-\lambda_{\mathrm{E}}, \varphi)$, and through $(1,1)$, $(1-\lambda_{\mathrm{E}}, \varphi)$. Based on the observation, the privacy-constrained operation region $\mathcal{R}_1^{\mathrm{P}}$ is determined by the parameters λ_{E} and φ as shown in Figure 4.3. Different from the privacy-constrained distributed Bayesian hypothesis testing problem, the privacy-constrained operation region $\mathcal{R}_1^{\mathrm{P}}$ for the privacy-constrained distributed Neyman-Pearson hypothesis testing problem is not convex!

Lemma 4.1. *For the privacy-constrained Neyman-Pearson hypothesis testing problem (4.12), it is sufficient to consider an optimal remote strategy ϕ_1^* which achieves the operation point $\boldsymbol{p}_1(\phi_1^*)$ on the boundary of the privacy-constrained operation region $\mathcal{R}_1^{\mathrm{P}}$.*

Proof. Define

$$a_1^*(m_1, h_{\mathrm{F}}, h) \triangleq \int_{\mathcal{Y}_2} \sum_{m_2 \in \mathcal{M}} p_{H_{\mathrm{F}}|M_1,M_2}^*(h_{\mathrm{F}}|m_1, m_2) p_{M_2|Y_2}^*(m_2|y_2) f_{Y_2|H}(y_2|h) dy_2. \tag{4.23}$$

The miss probability and false-alarm probability of fusion decision in (4.19) can be expressed in terms of detection probability and false-alarm probability of remote

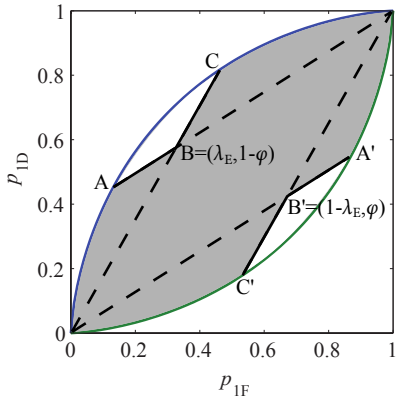


Figure 4.3: Illustration of the privacy-constrained operation region $\mathcal{R}_1^{\mathrm{P}}$ of the intercepted remote decision maker DM_1 when the hypothesis H and the remote decision M_1 are both binary random variables; the continuous random observation Y_1 is generated following $Y_1|H=0 \sim \mathcal{N}(0,1)$ or $Y_1|H=1 \sim \mathcal{N}(1,1)$; and the privacy leakage suppression guarantee satisfies $1-\hat{\partial}\mathcal{R}_1(\lambda_{\mathrm{E}}) < \varphi < 1-\lambda_{\mathrm{E}}$. The privacy leakage suppression constraint $p_{\mathrm{EM}}^{\min}(\phi_1) \geq \varphi$ leads to the line segments on the boundary: $\mathrm{A}-\mathrm{B}$, $\mathrm{B}-\mathrm{C}$, $\mathrm{A}'-\mathrm{B}'$, $\mathrm{B}'-\mathrm{C}'$. The operation points can be specified as: $\mathrm{B}=(\lambda_{\mathrm{E}}, 1-\varphi)$; A is an intersection point of $\hat{\partial}\mathcal{R}_1$ and the line through points B, $(1,1)$; C is an intersection point of $\hat{\partial}\mathcal{R}_1$ and the line through points B, $(0,0)$; $\mathrm{B}'=(1-\lambda_{\mathrm{E}}, \varphi)$; A' is an intersection point of $\check{\partial}\mathcal{R}_1$ and the line through points B', $(0,0)$; C' is an intersection point of $\check{\partial}\mathcal{R}_1$ and the line through points B', $(1,1)$.

decision M_1 respectively as

$$\begin{aligned}
p_{\mathrm{FM}}(\phi_1,\phi_2^*,\phi_{\mathrm{F}}^*) &= \sum_{m_1\in\mathcal{M}} a_1^*(m_1,0,1)\int_{\mathcal{Y}_1} p_{M_1|Y_1}(m_1|y_1) f_{Y_1|H}(y_1|1)dy_1 \\
&= a_1^*(0,0,1)p_{M_1|H}(0|1) + a_1^*(1,0,1)p_{M_1|H}(1|1) \\
&= a_1^*(0,0,1) + (a_1^*(1,0,1) - a_1^*(0,0,1))p_{1\mathrm{D}}(\phi_1), \\
p_{\mathrm{FF}}(\phi_1,\phi_2^*,\phi_{\mathrm{F}}^*) &= \sum_{m_1\in\mathcal{M}} a_1^*(m_1,1,0)\int_{\mathcal{Y}_1} p_{M_1|Y_1}(m_1|y_1) f_{Y_1|H}(y_1|0)dy_1 \\
&= a_1^*(0,1,0)p_{M_1|H}(0|0) + a_1^*(1,1,0)p_{M_1|H}(1|0) \\
&= a_1^*(0,1,0) + (a_1^*(1,1,0) - a_1^*(0,1,0))p_{1\mathrm{F}}(\phi_1).
\end{aligned} \tag{4.24}$$

Depending on the sign of the coefficient $a_1^*(1,0,1) - a_1^*(0,0,1)$, an optimal remote strategy ϕ_1^* of (4.19) maximizes or minimizes the detection probability of remote decision M_1 subject to that the corresponding false-alarm probability $p_{1\mathrm{F}}(\phi_1^*)$ satisfies $a_1^*(0,1,0) + (a_1^*(1,1,0) - a_1^*(0,1,0))p_{1\mathrm{F}}(\phi_1^*) = \lambda_{\mathrm{F}}$, i.e., the operation point

$\boldsymbol{p}_1(\phi_1^*) = (p_{1\mathrm{F}}(\phi_1^*), p_{1\mathrm{D}}(\phi_1^*))$ is on the upper or lower boundary of the privacy-constrained operation region $\mathcal{R}_1^{\mathrm{P}}$. □

Note that an operation point on the boundary of $\mathcal{R}_1^{\mathrm{P}}$ can be on the ROC/inverse ROC curves, i.e., it can be achieved by a deterministic LRT, or can be on the line segments $\mathrm{A}-\mathrm{B}$, $\mathrm{B}-\mathrm{C}$, $\mathrm{A}'-\mathrm{B}'$, $\mathrm{B}'-\mathrm{C}'$, i.e., it can be achieved by a randomized strategy of two deterministic LRTs. To verify the optimality of deterministic LRT for ϕ_1^*, the following discussion will focus on the remote decision strategies of DM_1 which achieve operation points on the line segments.

Given an optimal privacy-constrained distributed network $(\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}^*)$, instead of the PBPO problem of ϕ_1 in (4.19), the following PBPO problem of $(\phi_1, \phi_{\mathrm{F}})$ is considered as

$$(\phi_1^*, \phi_{\mathrm{F}}^*) = \begin{array}{ll} \arg\min & p_{\mathrm{FM}}(\phi_1, \phi_2^*, \phi_{\mathrm{F}}) \\ {\scriptstyle (\phi_1,\phi_{\mathrm{F}})\in\{\phi_1 | \boldsymbol{p}_1(\phi_1)\in\partial\mathcal{R}_1^{\mathrm{P}}\}\times\Phi_{\mathrm{F}}} & \\ \text{s.t.} & p_{\mathrm{FF}}(\phi_1, \phi_2^*, \phi_{\mathrm{F}}) = \lambda_{\mathrm{F}}. \end{array} \tag{4.25}$$

From Lemma 4.1, it is sufficient to consider the remote strategies which achieve operation points on the boundary of the privacy-constrained operation region $\mathcal{R}_1^{\mathrm{P}}$. The PBPO problem of $(\phi_1, \phi_{\mathrm{F}})$ can be reduced to an equivalent optimization problem of ϕ_1 by exploiting the optimality characteristics of the Neyman-Pearson hypothesis test at the FC as discussed in the following.

Given $(\phi_1, \phi_2) \in \Phi_1 \times \Phi_2$, define the fusion operation point achieved by a fusion strategy ϕ_{F} as

$$\boldsymbol{p}_{\mathrm{F}}(\phi_1, \phi_2, \phi_{\mathrm{F}}) \triangleq (p_{\mathrm{FF}}(\phi_1, \phi_2, \phi_{\mathrm{F}}), p_{\mathrm{FD}}(\phi_1, \phi_2, \phi_{\mathrm{F}})); \tag{4.26}$$

and define the operation region of the FC as

$$\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2) \triangleq \{\boldsymbol{p}_{\mathrm{F}}(\phi_1, \phi_2, \phi_{\mathrm{F}}) \,|\phi_{\mathrm{F}} \in \Phi_{\mathrm{F}}\}. \tag{4.27}$$

As shown in Property 2.2, the ROC curve (upper boundary) $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2)$ is concave and non-decreasing. The following property shows how $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2)$ relates with the given remote strategies (ϕ_1, ϕ_2).

Given remote strategies (ϕ_1, ϕ_2), the fusion observation likelihoods $p_{M_1,M_2|H}(\cdot|0)$ and $p_{M_1,M_2|H}(\cdot|1)$ are also known. Define a sort function

$$S : \{1, \ldots, ||\mathcal{M} \times \mathcal{M}||\} \to \mathcal{M} \times \mathcal{M}, \tag{4.28}$$

which maps an index $1 \le k \le 4$ to a remote decision sequence $S(k) \in \mathcal{M} \times \mathcal{M}$ with the k-th smallest likelihood ratio, i.e., there is a sorted likelihood-ratio chain (LRC) as

$$\frac{p_{M_1,M_2|H}(S(1)|0)}{p_{M_1,M_2|H}(S(1)|1)} \le \frac{p_{M_1,M_2|H}(S(2)|0)}{p_{M_1,M_2|H}(S(2)|1)} \le \frac{p_{M_1,M_2|H}(S(3)|0)}{p_{M_1,M_2|H}(S(3)|1)} \le \frac{p_{M_1,M_2|H}(S(4)|0)}{p_{M_1,M_2|H}(S(4)|1)}.$$

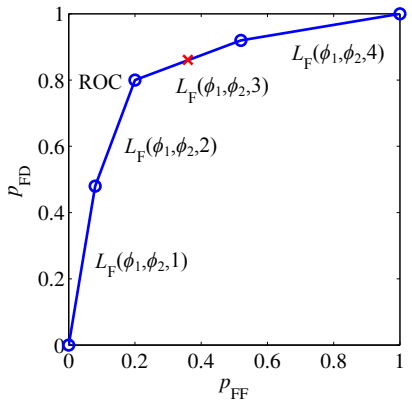


Figure 4.4: Illustration of the ROC curve $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2)$ of a fusion operation region. The order of the four line segments corresponds to the sorted LRC determined by the given remote strategies ϕ_1 and ϕ_2. The slope of the k-th line segment is determined by the k-th smallest fusion observation likelihood ratio. All circle points can be achieved by deterministic LRTs. Any other operation point on $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2)$, e.g., the red cross point, can be achieved by a randomized fusion strategy of two deterministic LRTs.

Property 4.1. *The ROC curve $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2)$ consists of $||\mathcal{M}\times\mathcal{M}|| = 4$ line segments. From $(0,0)$ to $(1,1)$, denote the k-th line segment by $L_{\mathrm{F}}(\phi_1,\phi_2,k)$, along which p_{FF} increases by $p_{M_1,M_2|H}(S(k)|0)$ while p_{FD} increases by $p_{M_1,M_2|H}(S(k)|1)$. An intersection point between two neighbor line segments of different slopes can be achieved by a deterministic LRT.*

Proof. From Property 2.2, all operation points on the ROC curve $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2)$ and achieved by deterministic fusion strategies can be achieved by deterministic LRTs in the form of

$$H_{\mathrm{F}} = \phi_{\mathrm{F}}(m_1,m_2) = \begin{cases} 0, & \text{if } \dfrac{p_{M_1,M_2|H}(m_1,m_2|0)}{p_{M_1,M_2|H}(m_1,m_2|1)} \geq t \\ 1, & \text{otherwise} \end{cases}.$$

Thus, Property 4.1 can be proved by characterizing the deterministic LRTs on the ROC curve $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2)$. These deterministic LRTs can be constructed by changing the test threshold t from 0 to $+\infty$. Note that the given remote strategies (ϕ_1,ϕ_2) have determined a sort function and the corresponding sorted LRC. For all test thresholds satisfying $\frac{p_{M_1,M_2|H}(S(i-1)|0)}{p_{M_1,M_2|H}(S(i-1)|1)} < t \leq \frac{p_{M_1,M_2|H}(S(i)|0)}{p_{M_1,M_2|H}(S(i)|1)}$, they lead to the same deterministic LRT with the decision region of hypothesis 1: $\{S(1),\ldots,S(i-1)\}$. In Figure 4.4, the ROC curve of a fusion operation region is illustrated. □

Given remote strategies (ϕ_1, ϕ_2), a fusion strategy ϕ_{F} achieves an operation point on the ROC curve $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2)$ with $p_{\mathrm{FF}}(\phi_1, \phi_2, \phi_{\mathrm{F}}) = c$. There is an abuse of notation to let $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2, c) = p_{\mathrm{FD}}(\phi_1, \phi_2, \phi_{\mathrm{F}})$. Then,

$$1 - \hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2, \lambda_{\mathrm{F}}) = \min_{\phi_{\mathrm{F}} \in \Phi_{\mathrm{F}}} p_{\mathrm{FM}}(\phi_1, \phi_2, \phi_{\mathrm{F}}) \quad \text{s.t. } p_{\mathrm{FF}}(\phi_1, \phi_2, \phi_{\mathrm{F}}) = \lambda_{\mathrm{F}}.$$

Suppose that the given remote strategies (ϕ_1, ϕ_2) lead to a sort function $S(\cdot)$. Let K denote the index such that the fusion operation point $(\lambda_{\mathrm{F}}, \hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2, \lambda_{\mathrm{F}}))$ is on the K-th line segment $L_{\mathrm{F}}(\phi_1, \phi_2, K)$. It follows from Property 4.1 that $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2, \lambda_{\mathrm{F}})$ can be specified in terms of $\boldsymbol{p}_1(\phi_1)$ and $\boldsymbol{p}_2(\phi_2)$ as

$$\begin{aligned} &\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2, \lambda_{\mathrm{F}}) \\ &= \sum_{i=1}^{K-1} p_{M_1,M_2|H}(S(i)|1) + \frac{p_{M_1,M_2|H}(S(K)|1)}{p_{M_1,M_2|H}(S(K)|0)} \left(\lambda_{\mathrm{F}} - \sum_{i=1}^{K-1} p_{M_1,M_2|H}(S(i)|0) \right), \end{aligned} \tag{4.29}$$

where $p_{M_1,M_2|H}$ is determined by $\boldsymbol{p}_1(\phi_1)$ and $\boldsymbol{p}_2(\phi_2)$.

Now, the PBPO problem of $(\phi_1, \phi_{\mathrm{F}})$ in (4.25) can be equivalently reformulated as the following optimization problem of ϕ_1

$$\phi_1^* = \underset{\{\phi_1 | \boldsymbol{p}_1(\phi_1) \in \partial\mathcal{R}_1^{\mathrm{P}}\}}{\arg\max} \hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2^*, \lambda_{\mathrm{F}}). \tag{4.30}$$

For any ϕ_1 which jointly with the given ϕ_2^* leads to the same sort function $S(\cdot)$ and the same index K, the objective in (4.30) can be specified in the same form as (4.29). Therefore, the optimization (4.30) can be divided into a set of optimizations: Every optimization maximizes a specified objective function of ϕ_1 in the form of (4.29) corresponding to a sort function $S(\cdot)$ and an index K over a subset of $\{\phi_1 | \boldsymbol{p}_1(\phi_1) \in \partial\mathcal{R}_1^{\mathrm{P}}\}$ which consists of remote strategies leading to the sort function $S(\cdot)$ and the index K.

To verify the optimality of deterministic LRT for ϕ_1^*, it is sufficient to focus on the remote decision strategies which achieve operation points on the boundary line segments $\mathrm{A} - \mathrm{B}$, $\mathrm{B} - \mathrm{C}$, $\mathrm{A}' - \mathrm{B}'$, and $\mathrm{B}' - \mathrm{C}'$. Note that these line segments are on the lines through the operation point $(0, 0)$ or $(1, 1)$. Given a remote strategy $\phi_2 \in \Phi_2$, the following lemmas show the monotonicity of $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2, \lambda_{\mathrm{F}})$ with increasing $p_{1\mathrm{F}}(\phi_1)$ along a line through the operation point $(0, 0)$ or $(1, 1)$ in the operation region $\mathcal{R}_1$.

Lemma 4.2. *For any $\phi_2 \in \Phi_2$ and $\lambda_{\mathrm{F}} < z < \hat{\partial}\mathcal{R}_1(\lambda_{\mathrm{F}})$, $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2, \lambda_{\mathrm{F}})$ is a non-increasing function of $p_{1\mathrm{F}}(\phi_1)$ along the line through operation points $(1, 1)$ and $(\lambda_{\mathrm{F}}, z)$ when $p_{1\mathrm{F}}(\phi_1) \leq \lambda_{\mathrm{F}}$; $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2, \lambda_{\mathrm{F}})$ is a non-decreasing function of $p_{1\mathrm{F}}(\phi_1)$ along the line through operation points $(0, 0)$ and $(\lambda_{\mathrm{F}}, z)$ when $p_{1\mathrm{F}}(\phi_1) \geq \lambda_{\mathrm{F}}$.*

Lemma 4.3. *For any $\phi_2 \in \Phi_2$ and $\breve{\partial}\mathcal{R}_1(1-\lambda_\mathrm{F}) < z < 1-\lambda_\mathrm{F}$, $\hat{\partial}\mathcal{R}_\mathrm{F}(\phi_1, \phi_2, \lambda_\mathrm{F})$ is a non-increasing function of $p_{1\mathrm{F}}(\phi_1)$ along the line through operation points $(1,1)$ and $(1-\lambda_\mathrm{F}, z)$ when $p_{1\mathrm{F}}(\phi_1) \leq 1-\lambda_\mathrm{F}$; $\hat{\partial}\mathcal{R}_\mathrm{F}(\phi_1, \phi_2, \lambda_\mathrm{F})$ is a non-decreasing function of $p_{1\mathrm{F}}(\phi_1)$ along the line through operation points $(0,0)$ and $(1-\lambda_\mathrm{F}, z)$ when $p_{1\mathrm{F}}(\phi_1) \geq 1-\lambda_\mathrm{F}$.*

The proof idea of Lemmas 4.2 and 4.3 is to specify $\hat{\partial}\mathcal{R}_\mathrm{F}(\phi_1, \phi_2, \lambda_\mathrm{F})$ in the form of (4.29) and to characterize its monotonicity along the line segments. The proof of Lemma 4.2 is shown in the appendix of this chapter. From these lemmas, the optimality of deterministic LRT for ϕ_1^* depends on the false-alarm probability upper bounds λ_E and λ_F, which is made concrete in the following theorems.

Theorem 4.2. *For the privacy-constrained Neyman-Pearson hypothesis testing problem (4.12) with $\lambda_\mathrm{F} = \lambda_\mathrm{E}$, it is sufficient to consider a deterministic LRT for ϕ_1^*.*

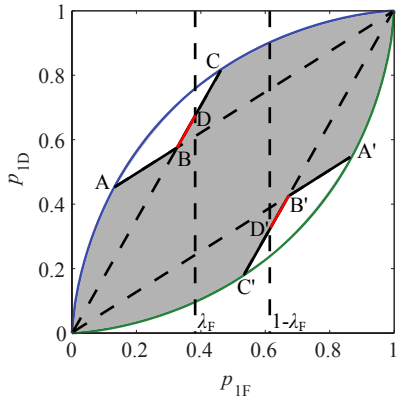
Proof. If $\lambda_\mathrm{F} = \lambda_\mathrm{E}$, Lemmas 4.2 and 4.3 lead to the following results:

$$\begin{aligned}
\mathrm{A} &= \operatorname*{arg\,max}_{\boldsymbol{p}_1(\phi_1) \in \mathrm{A}-\mathrm{B}} \hat{\partial}\mathcal{R}_\mathrm{F}(\phi_1, \phi_2^*, \lambda_\mathrm{F}); \\
\mathrm{C} &= \operatorname*{arg\,max}_{\boldsymbol{p}_1(\phi_1) \in \mathrm{B}-\mathrm{C}} \hat{\partial}\mathcal{R}_\mathrm{F}(\phi_1, \phi_2^*, \lambda_\mathrm{F}); \\
\mathrm{A}' &= \operatorname*{arg\,max}_{\boldsymbol{p}_1(\phi_1) \in \mathrm{A}'-\mathrm{B}'} \hat{\partial}\mathcal{R}_\mathrm{F}(\phi_1, \phi_2^*, \lambda_\mathrm{F}); \\
\mathrm{C}' &= \operatorname*{arg\,max}_{\boldsymbol{p}_1(\phi_1) \in \mathrm{B}'-\mathrm{C}'} \hat{\partial}\mathcal{R}_\mathrm{F}(\phi_1, \phi_2^*, \lambda_\mathrm{F}).
\end{aligned} \tag{4.31}$$

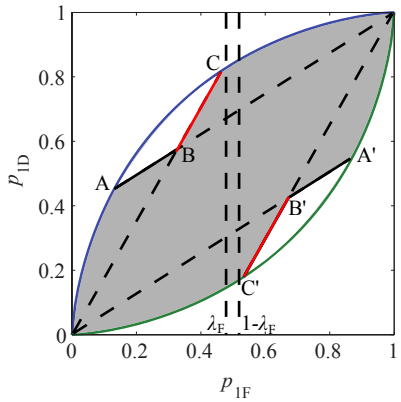
Note that the operation points A, C, A′, and C′ are on the ROC and inverse ROC curves of the operation region $\mathcal{R}_1$ and can be achieved by deterministic LRTs. Recall the optimization problem (4.30). It is sufficient to consider a deterministic LRT for ϕ_1^* which achieves an operation point in $\partial\mathcal{R}_1 \cap \partial\mathcal{R}_1^\mathrm{P}$. □

Theorem 4.3. *For the privacy-constrained Neyman-Pearson hypothesis testing problem (4.12) with $\lambda_\mathrm{F} \neq \lambda_\mathrm{E}$, an optimal remote strategy ϕ_1^* of the intercepted remote decision maker DM_1 can be a deterministic LRT or a randomized strategy of two deterministic LRTs. If ϕ_1^* is a randomized strategy, it achieves an operation point on the boundary line segments $\mathrm{A}-\mathrm{B}-\mathrm{C}$ with $p_{1\mathrm{F}}(\phi_1^*)$ between λ_F and λ_E, or an operation point on the boundary line segments $\mathrm{A}'-\mathrm{B}'-\mathrm{C}'$ with $p_{1\mathrm{F}}(\phi_1^*)$ between $1-\lambda_\mathrm{F}$ and $1-\lambda_\mathrm{E}$.*

Proof. If $\lambda_\mathrm{F} > \lambda_\mathrm{E}$ and considering the case shown in Figure 4.5a, Lemmas 4.2 and



(a)



(b)

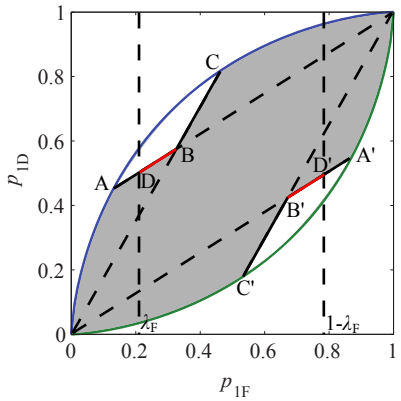
Figure 4.5: Possible cases of $\lambda_{\mathrm{F}} > \lambda_{\mathrm{E}}$. The monotonicity of $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2^*, \lambda_{\mathrm{F}})$ with increasing $p_{1\mathrm{F}}(\phi_1)$ along the red line segments is unknown.

4.3 lead to the following results:

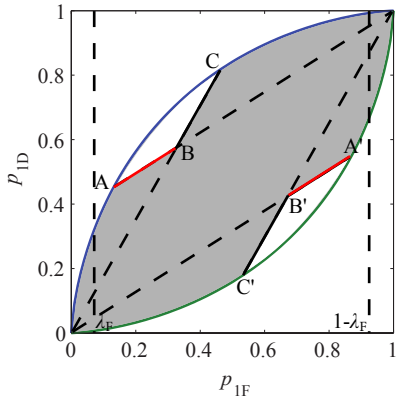
$$\begin{aligned}
\mathrm{A} &= \underset{\boldsymbol{p}_1(\phi_1)\in \mathrm{A}-\mathrm{B}}{\arg\max}\ \hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2^*, \lambda_{\mathrm{F}}); \\
\mathrm{C} &= \underset{\boldsymbol{p}_1(\phi_1)\in \mathrm{D}-\mathrm{C}}{\arg\max}\ \hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2^*, \lambda_{\mathrm{F}}); \\
\mathrm{A}' &= \underset{\boldsymbol{p}_1(\phi_1)\in \mathrm{A}'-\mathrm{B}'}{\arg\max}\ \hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2^*, \lambda_{\mathrm{F}}); \\
\mathrm{C}' &= \underset{\boldsymbol{p}_1(\phi_1)\in \mathrm{D}'-\mathrm{C}'}{\arg\max}\ \hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2^*, \lambda_{\mathrm{F}}).
\end{aligned} \tag{4.32}$$

If $\lambda_{\mathrm{F}} > \lambda_{\mathrm{E}}$ and considering the case shown in Figure 4.5b, Lemmas 4.2 and 4.3 lead to the following results:

$$\begin{aligned} \mathrm{A} &= \underset{\boldsymbol{p}_1(\phi_1)\in \mathrm{A}-\mathrm{B}}{\arg\max}\ \hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2^*, \lambda_{\mathrm{F}}); \\ \mathrm{A}' &= \underset{\boldsymbol{p}_1(\phi_1)\in \mathrm{A}'-\mathrm{B}'}{\arg\max}\ \hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2^*, \lambda_{\mathrm{F}}). \end{aligned} \tag{4.33}$$



(a)



(b)

Figure 4.6: Possible cases of $\lambda_{\mathrm{F}} < \lambda_{\mathrm{E}}$. The monotonicity of $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2^*, \lambda_{\mathrm{F}})$ with increasing $p_{1\mathrm{F}}(\phi_1)$ along the red line segments is unknown.

If $\lambda_{\mathrm{F}} < \lambda_{\mathrm{E}}$ and considering the case shown in Figure 4.6a, Lemmas 4.2 and 4.3

lead to the following results:

$$\begin{aligned}
\mathrm{A} &= \underset{\boldsymbol{p}_1(\phi_1)\in \mathrm{A-D}}{\arg\max}\ \hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2^*,\lambda_{\mathrm{F}});\\
\mathrm{C} &= \underset{\boldsymbol{p}_1(\phi_1)\in \mathrm{B-C}}{\arg\max}\ \hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2^*,\lambda_{\mathrm{F}});\\
\mathrm{A}' &= \underset{\boldsymbol{p}_1(\phi_1)\in \mathrm{A}'-\mathrm{D}'}{\arg\max}\ \hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2^*,\lambda_{\mathrm{F}});\\
\mathrm{C}' &= \underset{\boldsymbol{p}_1(\phi_1)\in \mathrm{B}'-\mathrm{C}'}{\arg\max}\ \hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2^*,\lambda_{\mathrm{F}}).
\end{aligned} \tag{4.34}$$

If $\lambda_{\mathrm{F}} < \lambda_{\mathrm{E}}$ and considering the case shown in Figure 4.6b, Lemmas 4.2 and 4.3 lead to the following results:

$$\begin{aligned}
\mathrm{C} &= \underset{\boldsymbol{p}_1(\phi_1)\in \mathrm{B-C}}{\arg\max}\ \hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2^*,\lambda_{\mathrm{F}});\\
\mathrm{C}' &= \underset{\boldsymbol{p}_1(\phi_1)\in \mathrm{B}'-\mathrm{C}'}{\arg\max}\ \hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2^*,\lambda_{\mathrm{F}}).
\end{aligned} \tag{4.35}$$

Along the line segments $\mathrm{A}-\mathrm{B}-\mathrm{C}$ with $p_{1\mathrm{F}}(\phi_1)$ between λ_{F} and λ_{E}, and along the line segments $\mathrm{A}'-\mathrm{B}'-\mathrm{C}'$ with $p_{1\mathrm{F}}(\phi_1)$ between $1-\lambda_{\mathrm{F}}$ and $1-\lambda_{\mathrm{E}}$, the monotonicity of $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2^*,\lambda_{\mathrm{F}})$ with increasing $p_{1\mathrm{F}}(\phi_1)$ is unknown. Therefore, it is sufficient to consider for ϕ_1^* a deterministic LRT which achieves an operation point in $\partial\mathcal{R}_1 \cap \partial\mathcal{R}_1^{\mathrm{P}}$ or a randomized strategy of two deterministic LRTs which achieves an operation point on the line segments along which the monotonicity of $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2^*,\lambda_{\mathrm{F}})$ with increasing $p_{1\mathrm{F}}(\phi_1)$ is unknown. □

4.3 Numerical Examples

In this section, hypothesis testing performances and privacy leakages of optimal privacy-constrained distributed Neyman-Pearson hypothesis testing network designs are shown and compared; and interesting observations are analyzed. For the two remote decision makers, the remote observations Y_1 and Y_2 are assumed to be generated following normal distributions:

$$\begin{aligned}
&Y_1|H=0 \sim \mathcal{N}(0,1),\ Y_2|H=0 \sim \mathcal{N}(0,1),\\
&Y_1|H=1 \sim \mathcal{N}(1,1),\ Y_2|H=1 \sim \mathcal{N}(1,1).
\end{aligned}$$

In Figure 4.7, it shows the trade-off between hypothesis testing performance and privacy leakage of optimal privacy-constrained distributed Neyman-Pearson hypothesis testing network designs where the false-alarm probability upper bounds of fusion decision and eavesdropper decision are set as $\lambda_{\mathrm{F}} = \lambda_{\mathrm{E}} = 0.5$. On the right hand side of the point in the black ellipse, as the privacy leakage suppression guarantee φ increases, the hypothesis testing performance measure $p_{\mathrm{FM}}(\phi_1^*,\phi_2^*,\phi_{\mathrm{F}}^*)$ also increases, i.e., a higher privacy leakage suppression guarantee is achieved at the

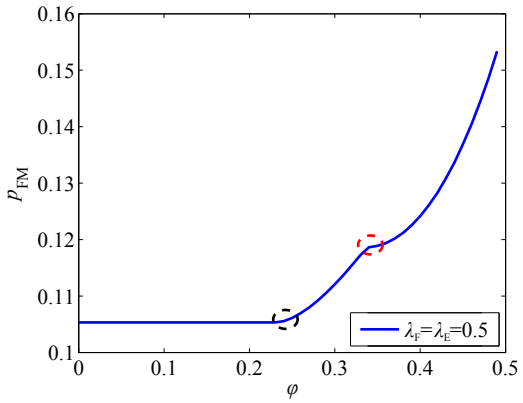


Figure 4.7: Trade-off between hypothesis testing performance and privacy leakage risk of optimal privacy-constrained distributed Neyman-Pearson hypothesis testing designs. The false-alarm probability upper bounds of fusion decision and eavesdropper decision are set as $\lambda_{\mathrm{F}} = \lambda_{\mathrm{E}} = 0.5$.

cost of a degraded hypothesis testing performance. On the left hand side of the point in the black ellipse, the hypothesis testing performance measure $p_{\mathrm{FM}}(\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}^*)$ does not change with the increase of φ. That is because an optimal remote strategy of DM_1 without a privacy leakage suppression constraint achieves an operation point in the privacy-constrained operation region $\mathcal{R}_1^{\mathrm{P}}$ when φ is lower than a certain value. On the two sides of the point in the red ellipse, it can be observed that the hypothesis testing performance measure $p_{\mathrm{FM}}(\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}^*)$ increases in different shapes. That is because the operation point $\boldsymbol{p}_1(\phi_1^*)$ achieved by an optimal privacy-constrained distributed Neyman-Pearson hypothesis testing design jumps between the two separated $\hat{\partial}\mathcal{R}_1$ segments on the upper boundary of the privacy-constrained operation region $\mathcal{R}_1^{\mathrm{P}}$.

In Figure 4.8, the curves correspond to three different settings on the false-alarm probability upper bounds of fusion decision and eavesdropper decision: $(\lambda_{\mathrm{F}} = 0.4, \lambda_{\mathrm{E}} = 0.5)$, $(\lambda_{\mathrm{F}} = 0.5, \lambda_{\mathrm{E}} = 0.5)$, and $(\lambda_{\mathrm{F}} = 0.6, \lambda_{\mathrm{E}} = 0.5)$. It illustrates how the hypothesis testing performance depends on the false-alarm probability upper bound λ_{F} of fusion decision. For each curve, trade-off between hypothesis testing performance and privacy leakage risk of optimal privacy-constrained distributed Neyman-Pearson hypothesis testing designs can be identified. Note that $\lambda_{\mathrm{E}} = 0.5$ in all settings. By fixing a value for φ, a privacy-constrained operation region $\mathcal{R}_1^{\mathrm{P}}$ is determined as shown in Figure 4.3. It can be observed that the hypothesis testing performance measure $p_{\mathrm{FM}}(\phi_1^*, \phi_2^*, \phi_{\mathrm{F}}^*)$ is higher corresponding to a lower value of λ_{F} when the value of φ is fixed. That is because the minimization of $p_{\mathrm{FM}}(\phi_1, \phi_2, \phi_{\mathrm{F}})$ is running over the same (privacy-constrained) operation regions $\mathcal{R}_1^P$ and $\mathcal{R}_2$ but under a lower upper bound on the false-alarm probability of fusion

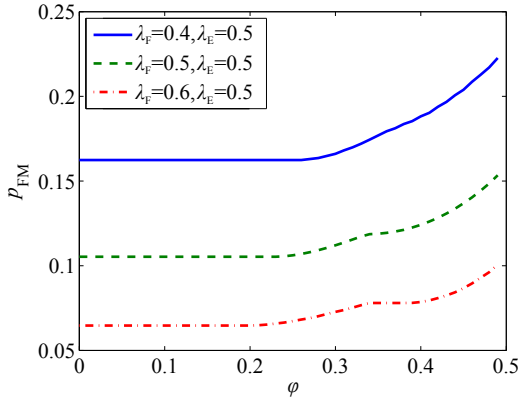


Figure 4.8: Comparison of hypothesis testing performances of optimal privacy-constrained distributed Neyman-Pearson hypothesis testing designs with different settings of false-alarm probability upper bounds of fusion decision and eavesdropper decision: $(\lambda_{\mathrm{F}} = 0.4, \lambda_{\mathrm{E}} = 0.5)$, $(\lambda_{\mathrm{F}} = 0.5, \lambda_{\mathrm{E}} = 0.5)$, and $(\lambda_{\mathrm{F}} = 0.6, \lambda_{\mathrm{E}} = 0.5)$.

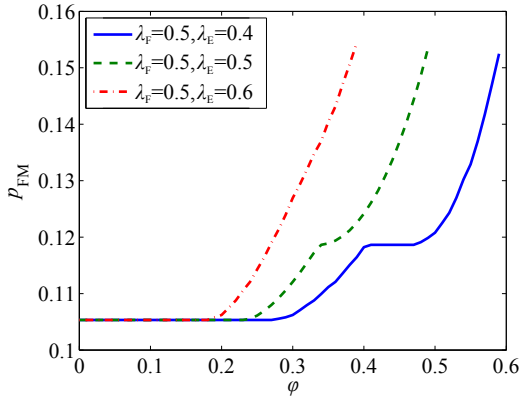


Figure 4.9: Comparison of hypothesis testing performances of optimal privacy-constrained distributed Neyman-Pearson hypothesis testing designs with different settings of false-alarm probability upper bounds of fusion decision and eavesdropper decision: $(\lambda_{\mathrm{F}} = 0.5, \lambda_{\mathrm{E}} = 0.4)$, $(\lambda_{\mathrm{F}} = 0.5, \lambda_{\mathrm{E}} = 0.5)$, and $(\lambda_{\mathrm{F}} = 0.5, \lambda_{\mathrm{E}} = 0.6)$.

decision $p_{\mathrm{FF}}(\phi_1, \phi_2, \phi_{\mathrm{F}})$.

In Figure 4.9, the curves correspond to three different settings on the false-alarm probability upper bounds of fusion decision and eavesdropper decision: ($\lambda_{\mathrm{F}} = 0.5, \lambda_{\mathrm{E}} = 0.4$), ($\lambda_{\mathrm{F}} = 0.5, \lambda_{\mathrm{E}} = 0.5$), and ($\lambda_{\mathrm{F}} = 0.5, \lambda_{\mathrm{E}} = 0.6$). It illustrates how the hypothesis testing performance depends on the false-alarm probability upper bound λ_{E} of eavesdropper decision. For each curve, trade-off between hypothesis testing performance and privacy leakage risk of optimal privacy-constrained distributed Neyman-Pearson hypothesis testing designs can be identified. By fixing a value for φ, a smaller value of λ_{E} means a larger privacy-constrained operation region $\mathcal{R}_1^{\mathrm{P}}$. Therefore, it can be identified in the plot that a not worse hypothesis testing performance is achieved with a lower value of λ_{E} when the value of φ is fixed.

4.4 Summary

In this chapter, the privacy-constrained distributed Neyman-Pearson hypothesis testing problem is formulated and studied. The privacy leakage suppression constraint leads to a non-convex privacy-constrained operation region for the intercepted remote decision maker. However, it is shown that the optimality of deterministic LRT still holds for the remote strategy of the intercepted decision maker when the same upper bound is set on the false-alarm probabilities of fusion decision and eavesdropper decision.

The discussion is based on the simple parallel model shown in Figure 4.1. If a general model as in Chapter 3 is used, the discussion will be much more complicated since the larger length of discrete random observation sequence of the FC/EVE and the requirement to always achieve the upper bound on the false-alarm probability of fusion/eavesdropper decision mean a much more complicated combinatorial problem to specify the objective/privacy-constrained operation region.

4.5 Appendix

In the following proof of Lemma 4.2, $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2, \lambda_{\mathrm{F}})$ needs to be specified in the form of (4.29). Therefore, it is necessary to identify possible sort functions and the corresponding sorted LRCs first.

Give a remote strategy ϕ_2 which satisfies $p_{2\mathrm{F}}(\phi_2) \leq p_{2\mathrm{D}}(\phi_2)$. If the remote strategy ϕ_1 is not fixed and satisfies $p_{1\mathrm{F}}(\phi_1) \leq p_{1\mathrm{D}}(\phi_1)$, a possible sort function and the corresponding sorted LRC are necessary to satisfy the inequalities $\frac{p_{1\mathrm{F}}(\phi_1)}{p_{1\mathrm{D}}(\phi_1)} \leq \frac{1-p_{1\mathrm{F}}(\phi_1)}{1-p_{1\mathrm{D}}(\phi_1)}$, $\frac{p_{2\mathrm{F}}(\phi_2)}{p_{2\mathrm{D}}(\phi_2)} \leq \frac{1-p_{2\mathrm{F}}(\phi_2)}{1-p_{2\mathrm{D}}(\phi_2)}$. The following two sort functions satisfy the inequalities and lead to the sorted LRCs as:

$$\begin{gathered} S(1) = (1,1),\ S(2) = (1,0),\ S(3) = (0,1),\ S(4) = (0,0); \\ \frac{p_{M_1,M_2|H}(1,1|0)}{p_{M_1,M_2|H}(1,1|1)} \leq \frac{p_{M_1,M_2|H}(1,0|0)}{p_{M_1,M_2|H}(1,0|1)} \leq \frac{p_{M_1,M_2|H}(0,1|0)}{p_{M_1,M_2|H}(0,1|1)} \leq \frac{p_{M_1,M_2|H}(0,0|0)}{p_{M_1,M_2|H}(0,0|1)}; \end{gathered} \tag{4.36}$$

and

$$\begin{gathered} S(1) = (1,1),\ S(2) = (0,1),\ S(3) = (1,0),\ S(4) = (0,0); \\ \frac{p_{M_1,M_2|H}(1,1|0)}{p_{M_1,M_2|H}(1,1|1)} \leq \frac{p_{M_1,M_2|H}(0,1|0)}{p_{M_1,M_2|H}(0,1|1)} \leq \frac{p_{M_1,M_2|H}(1,0|0)}{p_{M_1,M_2|H}(1,0|1)} \leq \frac{p_{M_1,M_2|H}(0,0|0)}{p_{M_1,M_2|H}(0,0|1)}. \end{gathered} \tag{4.37}$$

Give a remote strategy ϕ_2 which satisfies $p_{2\mathrm{F}}(\phi_2) \geq p_{2\mathrm{D}}(\phi_2)$. If the remote strategy ϕ_1 is not fixed and satisfies $p_{1\mathrm{F}}(\phi_1) \leq p_{1\mathrm{D}}(\phi_1)$, a possible sort function and the corresponding sorted LRC are necessary to satisfy the inequalities $\frac{p_{1\mathrm{F}}(\phi_1)}{p_{1\mathrm{D}}(\phi_1)} \leq \frac{1-p_{1\mathrm{F}}(\phi_1)}{1-p_{1\mathrm{D}}(\phi_1)}$, $\frac{p_{2\mathrm{F}}(\phi_2)}{p_{2\mathrm{D}}(\phi_2)} \geq \frac{1-p_{2\mathrm{F}}(\phi_2)}{1-p_{2\mathrm{D}}(\phi_2)}$. The following two sort functions satisfy the inequalities and lead to the sorted LRCs as:

$$\begin{gathered} S(1) = (1,0),\ S(2) = (0,0),\ S(3) = (1,1),\ S(4) = (0,1); \\ \frac{p_{M_1,M_2|H}(1,0|0)}{p_{M_1,M_2|H}(1,0|1)} \leq \frac{p_{M_1,M_2|H}(0,0|0)}{p_{M_1,M_2|H}(0,0|1)} \leq \frac{p_{M_1,M_2|H}(1,1|0)}{p_{M_1,M_2|H}(1,1|1)} \leq \frac{p_{M_1,M_2|H}(0,1|0)}{p_{M_1,M_2|H}(0,1|1)}; \end{gathered} \tag{4.38}$$

and

$$\begin{gathered} S(1) = (1,0),\ S(2) = (1,1),\ S(3) = (0,0),\ S(4) = (0,1); \\ \frac{p_{M_1,M_2|H}(1,0|0)}{p_{M_1,M_2|H}(1,0|1)} \leq \frac{p_{M_1,M_2|H}(1,1|0)}{p_{M_1,M_2|H}(1,1|1)} \leq \frac{p_{M_1,M_2|H}(0,0|0)}{p_{M_1,M_2|H}(0,0|1)} \leq \frac{p_{M_1,M_2|H}(0,1|0)}{p_{M_1,M_2|H}(0,1|1)}. \end{gathered} \tag{4.39}$$

Give a remote strategy ϕ_2 which satisfies $p_{2\mathrm{F}}(\phi_2) \leq p_{2\mathrm{D}}(\phi_2)$. If the remote strategy ϕ_1 is not fixed and satisfies $p_{1\mathrm{F}}(\phi_1) \geq p_{1\mathrm{D}}(\phi_1)$, a possible sort function and the corresponding sorted LRC are necessary to satisfy the inequalities $\frac{p_{1\mathrm{F}}(\phi_1)}{p_{1\mathrm{D}}(\phi_1)} \geq \frac{1-p_{1\mathrm{F}}(\phi_1)}{1-p_{1\mathrm{D}}(\phi_1)}$, $\frac{p_{2\mathrm{F}}(\phi_2)}{p_{2\mathrm{D}}(\phi_2)} \leq \frac{1-p_{2\mathrm{F}}(\phi_2)}{1-p_{2\mathrm{D}}(\phi_2)}$. The following two sort functions satisfy

the inequalities and lead to the sorted LRCs as:

$$S(1)=(0,1),\ S(2)=(1,1),\ S(3)=(0,0),\ S(4)=(1,0);$$
$$\frac{p_{M_1,M_2|H}(0,1|0)}{p_{M_1,M_2|H}(0,1|1)} \leq \frac{p_{M_1,M_2|H}(1,1|0)}{p_{M_1,M_2|H}(1,1|1)} \leq \frac{p_{M_1,M_2|H}(0,0|0)}{p_{M_1,M_2|H}(0,0|1)} \leq \frac{p_{M_1,M_2|H}(1,0|0)}{p_{M_1,M_2|H}(1,0|1)}; \tag{4.40}$$

and

$$S(1)=(0,1),\ S(2)=(0,0),\ S(3)=(1,1),\ S(4)=(1,0);$$
$$\frac{p_{M_1,M_2|H}(0,1|0)}{p_{M_1,M_2|H}(0,1|1)} \leq \frac{p_{M_1,M_2|H}(0,0|0)}{p_{M_1,M_2|H}(0,0|1)} \leq \frac{p_{M_1,M_2|H}(1,1|0)}{p_{M_1,M_2|H}(1,1|1)} \leq \frac{p_{M_1,M_2|H}(1,0|0)}{p_{M_1,M_2|H}(1,0|1)}. \tag{4.41}$$

Give a remote strategy ϕ_2 which satisfies $p_{2\mathrm{F}}(\phi_2) \geq p_{2\mathrm{D}}(\phi_2)$. If the remote strategy ϕ_1 is not fixed and satisfies $p_{1\mathrm{F}}(\phi_1) \geq p_{1\mathrm{D}}(\phi_1)$, a possible sort function and the corresponding sorted LRC are necessary to satisfy the inequalities $\frac{p_{1\mathrm{F}}(\phi_1)}{p_{1\mathrm{D}}(\phi_1)} \geq \frac{1-p_{1\mathrm{F}}(\phi_1)}{1-p_{1\mathrm{D}}(\phi_1)}$, $\frac{p_{2\mathrm{F}}(\phi_2)}{p_{2\mathrm{D}}(\phi_2)} \geq \frac{1-p_{2\mathrm{F}}(\phi_2)}{1-p_{2\mathrm{D}}(\phi_2)}$. The following two sort functions satisfy the inequalities and lead to the sorted LRCs as:

$$S(1)=(0,0),\ S(2)=(1,0),\ S(3)=(0,1),\ S(4)=(1,1);$$
$$\frac{p_{M_1,M_2|H}(0,0|0)}{p_{M_1,M_2|H}(0,0|1)} \leq \frac{p_{M_1,M_2|H}(1,0|0)}{p_{M_1,M_2|H}(1,0|1)} \leq \frac{p_{M_1,M_2|H}(0,1|0)}{p_{M_1,M_2|H}(0,1|1)} \leq \frac{p_{M_1,M_2|H}(1,1|0)}{p_{M_1,M_2|H}(1,1|1)}; \tag{4.42}$$

and

$$S(1)=(0,0),\ S(2)=(0,1),\ S(3)=(1,0),\ S(4)=(1,1);$$
$$\frac{p_{M_1,M_2|H}(0,0|0)}{p_{M_1,M_2|H}(0,0|1)} \leq \frac{p_{M_1,M_2|H}(0,1|0)}{p_{M_1,M_2|H}(0,1|1)} \leq \frac{p_{M_1,M_2|H}(1,0|0)}{p_{M_1,M_2|H}(1,0|1)} \leq \frac{p_{M_1,M_2|H}(1,1|0)}{p_{M_1,M_2|H}(1,1|1)}. \tag{4.43}$$

Proof of Lemma 4.2

Proof. Give a remote strategy ϕ_2 satisfying $p_{2\mathrm{F}}(\phi_2) \leq p_{2\mathrm{D}}(\phi_2)$ and a value z satisfying $\lambda_{\mathrm{F}} < z < \hat{\partial}\mathcal{R}_1(\lambda_{\mathrm{F}})$. The segment on the line through $(0,0)$ and $(\lambda_{\mathrm{F}}, z)$ in the operation region $\mathcal{R}_1$ is denoted by l_1 and is defined as

$$p_{1\mathrm{D}}(\phi_1) = \frac{z}{\lambda_{\mathrm{F}}} p_{1\mathrm{F}}(\phi_1) \text{ with } p_{1\mathrm{F}}(\phi_1) \geq \lambda_{\mathrm{F}};$$

and the segment on the line through $(1,1)$ and $(\lambda_{\mathrm{F}}, z)$ in the operation region $\mathcal{R}_1$ is denoted by l_2 and is defined as

$$p_{1\mathrm{D}}(\phi_1) = \frac{1-z}{1-\lambda_{\mathrm{F}}} p_{1\mathrm{F}}(\phi_1) + \frac{z-\lambda_{\mathrm{F}}}{1-\lambda_{\mathrm{F}}} \text{ with } p_{1\mathrm{F}}(\phi_1) \leq \lambda_{\mathrm{F}}.$$

Since these two line segments are above the line $p_{1\mathrm{D}}(\phi_1) = p_{1\mathrm{F}}(\phi_1)$, any operation point on the two line segments satisfies $p_{1\mathrm{F}}(\phi_1) \leq p_{1\mathrm{D}}(\phi_1)$. Therefore, the sort functions and corresponding sorted LRCs in (4.36) and (4.37) are possible.

Consider operation points on the two line segments and leading to the sort function in (4.36) and the index $K = 1$. Any such operation point has to satisfy $\lambda_{\mathrm{F}} \leq p_{M_1,M_2|H}(S(1)|0)$, i.e., $\lambda_{\mathrm{F}} \leq p_{1\mathrm{F}}(\phi_1)p_{2\mathrm{F}}(\phi_2)$. Therefore, any such operation point is on the line segment l_1. From (4.29), using ϕ_1 achieving a such operation point with the given ϕ_2,

$$\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2,\lambda_{\mathrm{F}}) = \frac{p_{M_1,M_2|H}(S(1)|1)}{p_{M_1,M_2|H}(S(1)|0)}\lambda_{\mathrm{F}} = \frac{p_{1\mathrm{D}}(\phi_1)p_{2\mathrm{D}}(\phi_2)}{p_{1\mathrm{F}}(\phi_1)p_{2\mathrm{F}}(\phi_2)}\lambda_{\mathrm{F}} = z\frac{p_{2\mathrm{D}}(\phi_2)}{p_{2\mathrm{F}}(\phi_2)}.$$

Note that the specified objective $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2,\lambda_{\mathrm{F}})$ does not depend on $p_{1\mathrm{F}}(\phi_1)$ or is non-decreasing with increasing $p_{1\mathrm{F}}(\phi_1)$ along l_1.

Consider operation points on the two line segments and leading to the sort function in (4.36) and the index $K = 2$. Any such operation point has to satisfy $p_{M_1,M_2|H}(S(1)|0) \leq \lambda_{\mathrm{F}} \leq \sum_{i=1}^{2} p_{M_1,M_2|H}(S(i)|0)$, i.e., $p_{1\mathrm{F}}(\phi_1)p_{2\mathrm{F}}(\phi_2) \leq \lambda_{\mathrm{F}} \leq p_{1\mathrm{F}}(\phi_1)$. Therefore, any such operation point is on the line segment l_1. From (4.29), using ϕ_1 achieving a such operation point with the given ϕ_2,

$$\begin{aligned}\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2,\lambda_{\mathrm{F}}) &= p_{M_1,M_2|H}(S(1)|1) + \frac{p_{M_1,M_2|H}(S(2)|1)}{p_{M_1,M_2|H}(S(2)|0)}\left(\lambda_{\mathrm{F}} - p_{M_1,M_2|H}(S(1)|0)\right)\\ &= \frac{z(p_{2\mathrm{D}}(\phi_2) - p_{2\mathrm{F}}(\phi_2))}{\lambda_{\mathrm{F}}(1-p_{2\mathrm{F}}(\phi_2))}p_{1\mathrm{F}}(\phi_1) + \frac{z(1-p_{2\mathrm{D}}(\phi_2))}{1-p_{2\mathrm{F}}(\phi_2)}.\end{aligned}$$

Note that the specified objective $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2,\lambda_{\mathrm{F}})$ is non-decreasing with increasing $p_{1\mathrm{F}}(\phi_1)$ along l_1.

Consider operation points on the two line segments and leading to the sort function in (4.36) and the index $K = 3$. Any such operation point has to satisfy $\sum_{i=1}^{2} p_{M_1,M_2|H}(S(i)|0) \leq \lambda_{\mathrm{F}} \leq \sum_{i=1}^{3} p_{M_1,M_2|H}(S(i)|0)$, i.e., $p_{1\mathrm{F}}(\phi_1) \leq \lambda_{\mathrm{F}} \leq p_{1\mathrm{F}}(\phi_1) + (1-p_{1\mathrm{F}}(\phi_1))p_{2\mathrm{F}}(\phi_2)$. Therefore, any such operation point is on the line segment l_2. From (4.29), using ϕ_1 achieving a such operation point with the given ϕ_2,

$$\begin{aligned}&\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2,\lambda_{\mathrm{F}})\\ &= \sum_{i=1}^{2} p_{M_1,M_2|H}(S(i)|1) + \frac{p_{M_1,M_2|H}(S(3)|1)}{p_{M_1,M_2|H}(S(3)|0)}\left(\lambda_{\mathrm{F}} - \sum_{i=1}^{2} p_{M_1,M_2|H}(S(i)|0)\right)\\ &= \frac{(1-z)(p_{2\mathrm{F}}(\phi_2) - p_{2\mathrm{D}}(\phi_2))}{(1-\lambda_{\mathrm{F}})p_{2\mathrm{F}}(\phi_2)}p_{1\mathrm{F}}(\phi_1) + \frac{z-\lambda_{\mathrm{F}}}{1-\lambda_{\mathrm{F}}} + \frac{1-z}{1-\lambda_{\mathrm{F}}}\frac{p_{2\mathrm{D}}(\phi_2)}{p_{2\mathrm{F}}(\phi_2)}\lambda_{\mathrm{F}}.\end{aligned}$$

Note that the specified objective $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2,\lambda_{\mathrm{F}})$ is non-increasing with increasing $p_{1\mathrm{F}}(\phi_1)$ along l_2.

Consider operation points on the two line segments and leading to the sort function in (4.36) and the index $K = 4$. Any such operation point has to satisfy $\sum_{i=1}^{3} p_{M_1,M_2|H}(S(i)|0) \leq \lambda_{\mathrm{F}} \leq 1$, i.e., $p_{1\mathrm{F}}(\phi_1) + (1-p_{1\mathrm{F}}(\phi_1))p_{2\mathrm{F}}(\phi_2) \leq \lambda_{\mathrm{F}} \leq 1$.

Therefore, any such operation point is on the line segment l_2. From (4.29), using ϕ_1 achieving a such operation point with the given ϕ_2,

$$\begin{aligned}
&\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2,\lambda_{\mathrm{F}}) \\
&= \sum_{i=1}^{3} p_{M_1,M_2|H}(S(i)|1) + \frac{p_{M_1,M_2|H}(S(4)|1)}{p_{M_1,M_2|H}(S(4)|0)} \left(\lambda_{\mathrm{F}} - \sum_{i=1}^{3} p_{M_1,M_2|H}(S(i)|0)\right) \\
&= 1 - (1-z)\frac{1-p_{2\mathrm{D}}(\phi_2)}{1-p_{2\mathrm{F}}(\phi_2)}.
\end{aligned}$$

Note that the specified objective $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2,\lambda_{\mathrm{F}})$ does not depend on $p_{1\mathrm{F}}(\phi_1)$ or is non-increasing with increasing $p_{1\mathrm{F}}(\phi_1)$ along l_2.

Consider operation points on the two line segments and leading to the sort function in (4.37) and the index $K = 1$. Any such operation point has to satisfy $\lambda_{\mathrm{F}} \leq p_{M_1,M_2|H}(S(1)|0)$, i.e., $\lambda_{\mathrm{F}} \leq p_{1\mathrm{F}}(\phi_1)p_{2\mathrm{F}}(\phi_2)$. Therefore, any such operation point is on the line segment l_1. From (4.29), using ϕ_1 achieving a such operation point with the given ϕ_2,

$$\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2,\lambda_{\mathrm{F}}) = \frac{p_{M_1,M_2|H}(S(1)|1)}{p_{M_1,M_2|H}(S(1)|0)}\lambda_{\mathrm{F}} = \frac{p_{1\mathrm{D}}(\phi_1)p_{2\mathrm{D}}(\phi_2)}{p_{1\mathrm{F}}(\phi_1)p_{2\mathrm{F}}(\phi_2)}\lambda_{\mathrm{F}} = z\frac{p_{2\mathrm{D}}(\phi_2)}{p_{2\mathrm{F}}(\phi_2)}.$$

Note that the specified objective $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2,\lambda_{\mathrm{F}})$ does not depend on $p_{1\mathrm{F}}(\phi_1)$ or is non-decreasing with increasing $p_{1\mathrm{F}}(\phi_1)$ along l_1.

Consider operation points on the two line segments and leading to the sort function in (4.37) and the index $K = 2$. Any such operation point has to satisfy $p_{M_1,M_2|H}(S(1)|0) \leq \lambda_{\mathrm{F}} \leq \sum_{i=1}^{2} p_{M_1,M_2|H}(S(i)|0)$, i.e., $p_{1\mathrm{F}}(\phi_1)p_{2\mathrm{F}}(\phi_2) \leq \lambda_{\mathrm{F}} \leq p_{2\mathrm{F}}(\phi_2)$. Note that a such operation point can be on l_1 or l_2. From (4.29), using ϕ_1 achieving a such operation point with the given ϕ_2,

$$\begin{aligned}
&\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2,\lambda_{\mathrm{F}}) \\
&= p_{M_1,M_2|H}(S(1)|1) + \frac{p_{M_1,M_2|H}(S(2)|1)}{p_{M_1,M_2|H}(S(2)|0)} \left(\lambda_{\mathrm{F}} - p_{M_1,M_2|H}(S(1)|0)\right) \\
&= \frac{p_{1\mathrm{D}}(\phi_1)p_{2\mathrm{D}}(\phi_2)p_{2\mathrm{F}}(\phi_2) + (1-p_{1\mathrm{D}}(\phi_1))p_{2\mathrm{D}}(\phi_2)\lambda_{\mathrm{F}} - p_{1\mathrm{F}}(\phi_1)p_{2\mathrm{D}}(\phi_2)p_{2\mathrm{F}}(\phi_2)}{(1-p_{1\mathrm{F}}(\phi_1))p_{2\mathrm{F}}(\phi_2)}.
\end{aligned}$$

For such operation points on l_1,

$$\frac{d\left(\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2,\lambda_{\mathrm{F}})\right)}{d\ p_{1\mathrm{F}}(\phi_1)} \geq 0,$$

where the inequality can be proved based on the inequality $\frac{z}{\lambda_{\mathrm{F}}}(1-p_{1\mathrm{F}}(\phi_1)) \geq 1-p_{1\mathrm{D}}(\phi_1)$ for any operation point on l_1. For such operation points on l_2,

$$\frac{d\left(\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1,\phi_2,\lambda_{\mathrm{F}})\right)}{d\ p_{1\mathrm{F}}(\phi_1)} = 0.$$

Therefore, the specified objective $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2, \lambda_{\mathrm{F}})$ is non-decreasing with increasing $p_{1\mathrm{F}}(\phi_1)$ along l_1 and non-increasing with increasing $p_{1\mathrm{F}}(\phi_1)$ along l_2.

Consider operation points on the two line segments and leading to the sort function in (4.37) and the index $K = 3$. Any such operation point has to satisfy $\sum_{i=1}^{2} p_{M_1,M_2|H}(S(i)|0) \leq \lambda_{\mathrm{F}} \leq \sum_{i=1}^{3} p_{M_1,M_2|H}(S(i)|0)$, i.e., $p_{2\mathrm{F}}(\phi_2) \leq \lambda_{\mathrm{F}} \leq p_{1\mathrm{F}}(\phi_1) + (1 - p_{1\mathrm{F}}(\phi_1))p_{2\mathrm{F}}(\phi_2)$. Note that a such operation point can be on l_1 or l_2. From (4.29), using ϕ_1 achieving a such operation point with the given ϕ_2,

$$\begin{aligned}
&\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2, \lambda_{\mathrm{F}}) \\
&= \sum_{i=1}^{2} p_{M_1,M_2|H}(S(i)|1) + \frac{p_{M_1,M_2|H}(S(3)|1)}{p_{M_1,M_2|H}(S(3)|0)} \left(\lambda_{\mathrm{F}} - \sum_{i=1}^{2} p_{M_1,M_2|H}(S(i)|0) \right) \\
&= \frac{p_{1\mathrm{F}}(\phi_1)p_{2\mathrm{D}}(\phi_2)(1 - p_{2\mathrm{F}}(\phi_2)) + p_{1\mathrm{D}}(\phi_1)(1 - p_{2\mathrm{D}}(\phi_2))(\lambda_{\mathrm{F}} - p_{2\mathrm{F}}(\phi_2))}{p_{1\mathrm{F}}(\phi_1)(1 - p_{2\mathrm{F}}(\phi_2))}.
\end{aligned}$$

For such operation points on l_1,

$$\frac{d\left(\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2, \lambda_{\mathrm{F}})\right)}{d\ p_{1\mathrm{F}}(\phi_1)} = 0.$$

For such operation points on l_2,

$$\frac{d\left(\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2, \lambda_{\mathrm{F}})\right)}{d\ p_{1\mathrm{F}}(\phi_1)} \leq 0.$$

Therefore, the specified objective $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2, \lambda_{\mathrm{F}})$ is non-decreasing with increasing $p_{1\mathrm{F}}(\phi_1)$ along l_1 and non-increasing with increasing $p_{1\mathrm{F}}(\phi_1)$ along l_2.

Consider operation points on the two line segments and leading to the sort function in (4.37) and the index $K = 4$. Any such operation point has to satisfy $\sum_{i=1}^{3} p_{M_1,M_2|H}(S(i)|0) \leq \lambda_{\mathrm{F}} \leq 1$, i.e., $p_{1\mathrm{F}}(\phi_1) + (1 - p_{1\mathrm{F}}(\phi_1))p_{2\mathrm{F}}(\phi_2) \leq \lambda_{\mathrm{F}} \leq 1$. Therefore, any such operation point is on the line segment l_2. From (4.29), using ϕ_1 achieving a such operation point with the given ϕ_2,

$$\begin{aligned}
&\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2, \lambda_{\mathrm{F}}) \\
&= \sum_{i=1}^{3} p_{M_1,M_2|H}(S(i)|1) + \frac{p_{M_1,M_2|H}(S(4)|1)}{p_{M_1,M_2|H}(S(4)|0)} \left(\lambda_{\mathrm{F}} - \sum_{i=1}^{3} p_{M_1,M_2|H}(S(i)|0) \right) \\
&= 1 - (1 - z)\frac{1 - p_{2\mathrm{D}}(\phi_2)}{1 - p_{2\mathrm{F}}(\phi_2)}.
\end{aligned}$$

Note that the specified objective $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2, \lambda_{\mathrm{F}})$ does not depend on $p_{1\mathrm{F}}(\phi_1)$ or is non-increasing with increasing $p_{1\mathrm{F}}(\phi_1)$ along l_2.

Give a remote strategy ϕ_2 satisfying $p_{2\mathrm{F}}(\phi_2) \geq p_{2\mathrm{D}}(\phi_2)$. Define the same line segments l_1 and l_2. The sort functions and corresponding sorted LRCs in (4.38)

and (4.39) are possible. Following similar analysis, the same monotonicity can be identified for $\hat{\partial}\mathcal{R}_{\mathrm{F}}(\phi_1, \phi_2, \lambda_{\mathrm{F}})$ with increasing $p_{1\mathrm{F}}(\phi_1)$ along l_1 or l_2. □

Chapter 5

Smart Meter Privacy in the Presence of a Renewable Source

In a smart grid, high-resolution readings of smart meters enable a better monitoring and control of the electric grid but also mean severer potential privacy leakages. In face of the smart meter privacy problem, a general privacy-preserving idea is to distort the meter readings to hide the real energy demands or the energy consumption behaviors. It can be realized through simply adding noises to the meter readings without changing the energy flows. Recently, integration of renewable energy sources (RESs) or energy storages (ESs) in smart grids provides another noise sources which change the energy flows. In this chapter, the smart meter privacy problem is considered in the presence of an ideal RES. Information-theoretic measures are used to assess the adversarial hypothesis testing privacy leakages. Fundamental bounds on the asymptotic privacy-preserving performances are to be studied.

5.1 System Model

The setup of the considered smart meter privacy problem is shown in Figure 5.1. The private consumer behavior is modeled by the binary hypothesis H which can be h_0 or h_1, e.g., following Ramadan or not. Let p_0 and p_1 denote the prior probabilities of hypotheses h_0 and h_1, respectively. W.l.o.g., it is assumed that p_0, $p_1 \neq 0$. In this chapter, the short notation $\cdot|h_j$ is used instead of $\cdot|H = h_j$, $j \in \{0, 1\}$, 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 i.i.d. generated according to $p_{X|h_0}$ (resp. $p_{X|h_1}$) where $p_{X|h_0}$ and $p_{X|h_1}$ satisfy $0 < \mathrm{D}(p_{X|h_0}||p_{X|h_1}) < +\infty$. The finite energy demand alphabet is assumed to satisfy $\mathcal{X} \subset \mathbb{Z}$; $\min \mathcal{X} \geq 0$; and $\max \mathcal{X} < +\infty$. At any time slot i, the energy management unit (EMU) follows an energy management policy γ_i to determine the (random) energy supply Y_i from the energy provider (EP) based on the demands x^i, the supplies y^{i-1}, and the correct

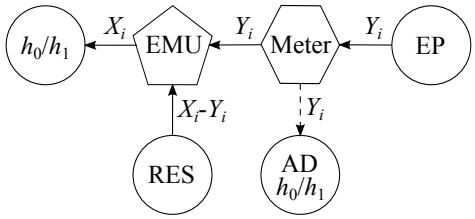


Figure 5.1: The smart meter privacy problem in the presence of a renewable energy source (RES), where energy and information flows are represented by solid and dashed arrows, respectively. The binary behavior hypothesis realizations are denoted by h_0 and h_1. At a time slot i, the random energy demand X_i is i.i.d. generated conditioned on hypothesis h_0 or h_1; the random energy supply Y_i from the energy provider (EP) is determined by the energy management unit (EMU); and the energy supply from the renewable energy source is $X_i - Y_i$. Based on a sequence of meter readings y^n, the adversary (AD) makes an inference h_0 or h_1 on the behavior.

hypothesis h as $Y_i = \gamma_i(x^i, y^{i-1}, h)$. A policy γ_i can also be represented by the corresponding conditional p.m.f. $p_{Y_i|X^i,Y^{i-1},H}$. Let $\mathcal{Y} \triangleq \{0, \ldots, \max \mathcal{X}\}$ denote the finite energy supply alphabet from the EP at any time slot with $\mathcal{X} \subseteq \mathcal{Y} \subset \mathbb{Z}$. A policy γ_i has to satisfy the following instantaneous constraint

$$p_{Y_i|X^i,Y^{i-1},h_j}(y_i|x^i, y^{i-1}) = 0, \text{ if } y_i > x_i, \text{ for all } j \in \{0, 1\}, \tag{5.1}$$

which 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. It is assumed that the RES has an average energy generation rate of s and is equipped with a sufficiently large ES. If the following average energy constraint is satisfied over a sufficiently large n-slot time horizon

$$\mathrm{E}\left[\frac{1}{n}\sum_{i=1}^{n}(X_i - Y_i)\middle| h_j\right] \leq s, \ j = 0, 1, \tag{5.2}$$

the availability of renewable energy supplies is guaranteed almost surely. An energy management policy over an n-slot time horizon that satisfies (5.2) is denoted by $\gamma^n(s)$. Let $\Gamma^n(s)$ denote the set of energy management policies over an n-slot time horizon and satisfying (5.2), i.e., $\gamma^n(s) \in \Gamma^n(s)$.

An adversary (AD), which can be the EP, is assumed to have access to the meter readings y^n, and to be fully informed about the hypothesis prior probability distribution, the energy demand statistics, as well as the used energy management policy, i.e., the AD knows p_0, p_1, $p_{X^n|h_0}$, $p_{X^n|h_1}$, $\gamma^n(s)$, and therefore the resulting energy supply statistics $p_{Y^n|h_0}$, $p_{Y^n|h_1}$. Further, the informed AD is assumed to make an optimal hypothesis test on the consumer behavior. The smart me-

ter privacy leakage is measured through a probability of error in the adversarial hypothesis testing.

In the following, the hypothesis testing model of smart meter privacy leakage is specified as a Neyman-Pearson hypothesis testing problem or a Bayesian hypothesis testing problem. The corresponding optimal privacy-preserving performance will be characterized in the asymptotic regime.

5.2 Adversarial Neyman-Pearson Hypothesis Testing

Here, the smart meter privacy leakage is modeled as a Neyman-Pearson hypothesis test by the informed AD on the consumer behavior. Given an energy management policy $\gamma^n(s)$ and the resulting $p_{Y^n|h_0}$, $p_{Y^n|h_1}$, the minimal Type II probability of error (miss probability) of the AD under an upper bound constraint on the Type I probability of error (false-alarm probability) is defined 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 $\mathcal{A}_n$ and $\mathcal{A}_n^c$ denote the decision regions for h_0 and h_1 of the AD, respectively. The design objective of the privacy-preserving EMU is to maximize the probability of error of the AD. More specifically, for a given RES energy generation rate s, the optimal energy management policy for the EMU achieves the maximum minimal Type II probability of error subject to Type I probability of error constraint, i.e.,

$$\beta(n,\varepsilon,s) \triangleq \max_{\gamma^n(s)\in\Gamma^n(s)}\{\beta(n,\varepsilon,\gamma^n(s))\}. \tag{5.3}$$

The main objective of this work is to characterize the fundamental bounds on the privacy-preserving performances. Note that $\beta(n,\varepsilon,s)$ is a non-increasing function of the meter reading length n. The following discussion focuses 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 a Kullback-Leibler divergence rate expression $\theta(s)$ as

$$\theta(s) \triangleq \inf_{k\in\mathbb{Z}_+}\left\{\inf_{\gamma^k(s)\in\Gamma^k(s)}\left\{\frac{1}{k}\mathrm{D}(p_{Y^k|h_0}||p_{Y^k|h_1})\right\}\right\}. \tag{5.4}$$

The operational meaning of $\theta(s)$ is shown later.

Lemma 5.1. *The infimum over k in the definition of $\theta(s)$ is taken at the limit $k\to\infty$:*

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

Proof. First, the sequence of $\inf_{\gamma^k(s)\in\Gamma^k(s)}\left\{\mathrm{D}(p_{Y^k|h_0}||p_{Y^k|h_1})\right\}$ is shown to be *sub-additive*. Given any n, $l\in\mathbb{Z}_+$, let $(\gamma^n(s),\gamma^l(s))$ denote an energy management

policy, which independently uses $\gamma^n(s)$ over the first n slots, and $\gamma^l(s)$ over the remaining l slots. Therefore, $(\gamma^n(s), \gamma^l(s))$ satisfies the average energy constraint over an $(n+l)$-slot time horizon. It follows that

$$\begin{aligned}
&\inf_{\gamma^{n+l}(s)\in\Gamma^{n+l}(s)} \left\{\mathrm{D}(p_{Y^{n+l}|h_0}||p_{Y^{n+l}|h_1})\right\} \\
\leq\ &\inf_{(\gamma^n(s),\gamma^l(s))\in\Gamma^n(s)\times\Gamma^l(s)} \left\{\mathrm{D}(p_{Y^{n+l}|h_0}||p_{Y^{n+l}|h_1})\right\} \\
=\ &\inf_{(\gamma^n(s),\gamma^l(s))\in\Gamma^n(s)\times\Gamma^l(s)} \left\{\mathrm{D}(p_{Y^{n}|h_0}||p_{Y^{n}|h_1}) + \mathrm{D}(p_{Y^{l}|h_0}||p_{Y^{l}|h_1})\right\} \\
=\ &\inf_{\gamma^n(s)\in\Gamma^n(s)} \left\{\mathrm{D}(p_{Y^{n}|h_0}||p_{Y^{n}|h_1})\right\} + \inf_{\gamma^l(s)\in\Gamma^l(s)} \left\{\mathrm{D}(p_{Y^{l}|h_0}||p_{Y^{l}|h_1})\right\}.
\end{aligned}$$

Then, Fekete's lemma [13, Lemma 11.2] leads to

$$\lim_{k\to\infty} \inf_{\gamma^k(s)\in\Gamma^k(s)} \left\{\frac{1}{k}\mathrm{D}(p_{Y^k|h_0}||p_{Y^k|h_1})\right\} = \inf_{k\in\mathbb{Z}_+} \left\{\inf_{\gamma^k(s)\in\Gamma^k(s)} \left\{\frac{1}{k}\mathrm{D}(p_{Y^k|h_0}||p_{Y^k|h_1})\right\}\right\}.$$

□

In the following theorem, 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 5.1. *Given $s > 0$,*

$$\limsup_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta(n,\varepsilon,s)} \leq \theta(s),\ \forall \varepsilon \in (0,1), \tag{5.5}$$

and

$$\lim_{\varepsilon\to 1} \liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta(n,\varepsilon,s)} \geq \theta(s). \tag{5.6}$$

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 (5.3) and Stein's lemma [12, Theorem 11.8.3], it follows that

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

for all $\varepsilon \in (0,1)$. For $k(l-1) < n \leq kl$, the following inequality holds:

$$\beta(kl,\varepsilon,s) \leq \beta(n,\varepsilon,s) \leq \beta(k(l-1),\varepsilon,s).$$

It follows that

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

for all $\varepsilon \in (0,1)$, $k \in \mathbb{Z}_+$, and $\gamma^k(s)$. Therefore, the upper bound holds:

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

Let

$$\varepsilon' \triangleq \sup_{k\in\mathbb{Z}_+} \left\{ \sup_{\gamma^k(s)\in\Gamma^k(s)} \left\{ p_{Y^k|h_0} \left(\left\{ y^k \left| \log \frac{p_{Y^k|h_0}(y^k)}{p_{Y^k|h_1}(y^k)} < \mathrm{D}\left(p_{Y^k|h_0}||p_{Y^k|h_1}\right) \right. \right\} \right) \right\} \right\}.$$

If $\varepsilon' < 1$, 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 $\beta(n,\varepsilon',s)$. If the AD uses the following hypothesis testing strategy

$$\mathcal{A}_n = \left\{ y^n \left| \frac{1}{n} \log \frac{p^*_{Y^n|h_0}(y^n)}{p^*_{Y^n|h_1}(y^n)} \geq t(n) \right. \right\}, \tag{5.7}$$

with the test threshold

$$t(n) = \frac{1}{n} \mathrm{D}(p^*_{Y^n|h_0}||p^*_{Y^n|h_1}), \tag{5.8}$$

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 testing strategy in (5.7) is not necessarily optimal for the AD, the definition of the maximum minimal Type II probability of error implies that

$$\beta(n,\varepsilon',s) \leq p^*_{Y^n|h_1}(\mathcal{A}_n). \tag{5.9}$$

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

$$p^*_{Y^n|h_1}(\mathcal{A}_n) \leq \exp(-nt(n)). \tag{5.10}$$

The inequalities (5.9) and (5.10) jointly lead to

$$\beta(n,\varepsilon',s) \leq \exp(-nt(n)) \leq \exp\left(-n \inf_{\gamma^n(s)\in\Gamma^n(s)} \left\{ \frac{1}{n} \mathrm{D}(p_{Y^n|h_0}||p_{Y^n|h_1}) \right\} \right),$$

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

$$\frac{1}{n} \log \frac{1}{\beta(n,\varepsilon',s)} \geq \inf_{\gamma^n(s)\in\Gamma^n(s)} \left\{ \frac{1}{n} \mathrm{D}(p_{Y^n|h_0}||p_{Y^n|h_1}) \right\}.$$

In the asymptotic regime as $n \to \infty$, it follows that

$$\liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta(n,\varepsilon',s)} \geq \lim_{n\to\infty} \inf_{\gamma^n(s)\in\Gamma^n(s)} \left\{ \frac{1}{n} \mathrm{D}(p_{Y^n|h_0}||p_{Y^n|h_1}) \right\} = \theta(s),$$

where the last equality follows from Lemma 5.1. Note that $\liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta(n,\varepsilon,s)}$ is a monotone non-decreasing function of ε. Then the lower bound holds:

$$\lim_{\varepsilon\to 1} \liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta(n,\varepsilon,s)} \geq \liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta(n,\varepsilon',s)} \geq \theta(s). \tag{5.11}$$

If $\varepsilon' = 1$, 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 $\beta(n, 1-\varphi, s)$, where $\varphi > 0$ can be arbitrarily small such that the Type I probability of error corresponding to the hypothesis testing strategy in (5.7) satisfies the upper bound constraint $1-\varphi$. It follows that

$$\beta(n, 1-\varphi, s) \leq p^*_{Y^n|h_1}(\mathcal{A}_n). \tag{5.12}$$

Following the same arguments, the lower bound can be proved as

$$\lim_{\varepsilon\to 1} \liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta(n,\varepsilon,s)} \geq \liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta(n,1-\varphi,s)} \geq \theta(s). \tag{5.13}$$

□

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 5.1. *Given $s > 0$,*

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

Remark 5.1. *Given $s > 0$, letting $\varepsilon \to 1$ represents the worst privacy leakage scenario under the adversarial Neyman-Pearson hypothesis testing, i.e., $\theta(s)$ can be used as a privacy-preserving guarantee.*

Generally, the evaluation of the asymptotic optimal privacy-preserving performance $\theta(s)$ and the design of optimal privacy-preserving energy management policies are difficult. In the following, the asymptotic privacy-preserving performances of two special energy management policies are characterized in the worst case scenario, i.e., $\varepsilon \to 1$.

Memoryless hypothesis-aware policy

At time slot i, a simple EMU can apply 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 $Y_i = \pi_i(x_i, h)$. The following instantaneous constraint has to be satisfied by a policy π_i:

$$p_{Y_i|X_i,h_j}(y_i|x_i) = 0, \text{ if } y_i > x_i, \text{ for all } j \in \{0,1\}. \tag{5.14}$$

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 (5.2), it is denoted by $\pi^n(s)$. Let $\Pi^n(s)$ denote the set of memoryless hypothesis-aware policies over an n-slot time horizon and satisfying (5.2), i.e., $\pi^n(s) \in \Pi^n(s)$. 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

$$\beta_{\mathrm{L}}(n, \varepsilon, s) \triangleq \max_{\pi^n(s) \in \Pi^n(s)} \{\beta(n, \varepsilon, \pi^n(s))\}. \tag{5.15}$$

Define a Kullback-Leibler divergence rate $\theta_{\mathrm{L}}(s)$ similar to $\theta(s)$ as

$$\theta_{\mathrm{L}}(s) \triangleq \inf_{k \in \mathbb{Z}_+} \left\{ \inf_{\pi^k(s) \in \Pi^k(s)} \left\{ \frac{1}{k} \mathrm{D}(p_{Y^k|h_0} || p_{Y^k|h_1}) \right\} \right\}. \tag{5.16}$$

Following a similar proof as Theorem 5.1, the asymptotic exponential decay rate of the maximum minimal Type II probability of error can be specified by the Kullback-Leibler divergence rate expression $\theta_{\mathrm{L}}(s)$ when the EMU uses the optimal privacy-preserving memoryless hypothesis-aware policy.

Corollary 5.2. *Given $s > 0$,*

$$\lim_{\varepsilon \to 1} \lim_{n \to \infty} \frac{1}{n} \log \frac{1}{\beta_{\mathrm{L}}(n, \varepsilon, s)} = \theta_{\mathrm{L}}(s). \tag{5.17}$$

It is shown in the following that the asymptotic exponential decay rate of the maximum minimal Type II probability of error can also be characterized by a single-letter Kullback-Leibler divergence expression.

Given $\bar{s}$, $\tilde{s} > 0$, define a single-letter Kullback-Leibler divergence $\phi(\bar{s}, \tilde{s})$ as

$$\phi(\bar{s}, \tilde{s}) \triangleq \min_{(p_{Y|X,h_0}, p_{Y|X,h_1}) \in \mathcal{P}(\bar{s}, \tilde{s})} \left\{ \mathrm{D}(p_{Y|h_0} || p_{Y|h_1}) \right\}, \tag{5.18}$$

where the minimization is over the convex domain

$$\mathcal{P}(\bar{s}, \tilde{s}) \triangleq \left\{ (p_{Y|X,h_0}, p_{Y|X,h_1}) \left| \begin{array}{c} \mathrm{E}[X - Y|h_0] \le \bar{s} \\ \mathrm{E}[X - Y|h_1] \le \tilde{s} \\ p_{Y|X,h_0}(y|x) = 0, \text{ if } y > x \\ p_{Y|X,h_1}(y|x) = 0, \text{ if } y > x \end{array} \right. \right\}.$$

In the definition of $\mathcal{P}(\bar{s}, \tilde{s})$, $\mathrm{E}[X - Y|h_0] \le \bar{s}$ denotes the single-slot average energy constraint under hypothesis h_0; $\mathrm{E}[X - Y|h_1] \le \tilde{s}$ 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 5.2. *$\phi(\bar{s},\tilde{s})$ is a non-increasing, continuous, and jointly convex function for $\bar{s}>0$ and $\tilde{s}>0$.*

Proof. The non-increasing property of $\phi(\bar{s},\tilde{s})$ is self-evident. On the two-dimensional convex open set of $\bar{s}>0$, $\tilde{s}>0$, its continuity will follow from the convexity [2]. Therefore, only the convexity is proved here. Assume that $(p^{(1)}_{Y|X,h_0}, p^{(1)}_{Y|X,h_1})$ leads to $\phi(\bar{s}_1,\tilde{s}_1) = \mathrm{D}(p^{(1)}_{Y|h_0}||p^{(1)}_{Y|h_1})$ and $(p^{(2)}_{Y|X,h_0}, p^{(2)}_{Y|X,h_1})$ leads to $\phi(\bar{s}_2,\tilde{s}_2) = \mathrm{D}(p^{(2)}_{Y|h_0}||p^{(2)}_{Y|h_1})$. For all $0\le\lambda\le 1$,

$$\begin{aligned}
&\lambda\phi(\bar{s}_1,\tilde{s}_1)+(1-\lambda)\phi(\bar{s}_2,\tilde{s}_2)\\
&=\lambda\mathrm{D}(p^{(1)}_{Y|h_0}||p^{(1)}_{Y|h_1})+(1-\lambda)\mathrm{D}(p^{(2)}_{Y|h_0}||p^{(2)}_{Y|h_1})\\
&\ge \mathrm{D}(\lambda p^{(1)}_{Y|h_0}+(1-\lambda)p^{(2)}_{Y|h_0}||\lambda p^{(1)}_{Y|h_1}+(1-\lambda)p^{(2)}_{Y|h_1})\\
&\ge \phi(\lambda\bar{s}_1+(1-\lambda)\bar{s}_2,\lambda\tilde{s}_1+(1-\lambda)\tilde{s}_2),
\end{aligned}$$

where the first inequality follows from the convexity of Kullback-Leibler divergence; and the second follows from the definition of $\phi(\bar{s},\tilde{s})$ in (5.18). □

The properties of $\phi(\bar{s},\tilde{s})$ in Lemma 5.2 will be used to prove the equivalence of the Kullback-Leibler divergence rate $\theta_{\mathrm{L}}(s)$ and the single-letter Kullback-Leibler divergence $\phi(s,s)$ as shown in the following theorem.

Theorem 5.2. *Given $s>0$,*

$$\theta_{\mathrm{L}}(s)=\phi(s,s). \tag{5.19}$$

Proof. For any $k\in\mathbb{Z}_+$, $\pi^k(s)$, and the resulting $p_{Y^k|h_0}$, $p_{Y^k|h_1}$, the Kullback-Leibler divergence rate $\frac{1}{k}\mathrm{D}\left(p_{Y^k|h_0}||p_{Y^k|h_1}\right)$ is lower bounded by $\phi(s,s)$ as

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

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, $\theta_{\mathrm{L}}(s)$ is lower bounded by $\phi(s, s)$:

$$\theta_{\mathrm{L}}(s) = \inf_{k \in \mathbb{Z}_+} \left\{ \inf_{\pi^k(s) \in \Pi^k(s)} \left\{ \frac{1}{k} \mathrm{D}(p_{Y^k|h_0} || p_{Y^k|h_1}) \right\} \right\} \geq \phi(s, s). \tag{5.20}$$

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 (5.16), it follows that

$$\theta_{\mathrm{L}}(s) \leq \phi(s, s). \tag{5.21}$$

Alternatively, the inequality (5.21) 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 (5.20) and (5.21) jointly lead to Theorem 5.2. □

Remark 5.2. *Given $s > 0$, the asymptotic exponential decay rate of the maximum minimal Type II probability of error $\lim_{\varepsilon \to 1} \lim_{n \to \infty} \frac{1}{n} \log \frac{1}{\beta_{\mathrm{L}}(n, \varepsilon, s)}$ can be achieved by a memoryless hypothesis-aware policy which uses time-invariant single-slot policy $(p^*_{Y|X,h_0}, p^*_{Y|X,h_1})$ corresponding to the optimizer of $\phi(s, s)$ at all time slots.*

Hypothesis-unaware policy with memory

In this section, a "counter" case is considered: The EMU stores the information of all past demands and supplies while it does not know the correct hypothesis. 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 $Y_i = \rho_i(x^i, y^{i-1})$. The following instantaneous constraint has to be satisfied by a policy ρ_i:

$$p_{Y_i|X^i,Y^{i-1}}(y_i|x^i, y^{i-1}) = 0, \text{ if } y_i > x_i. \tag{5.22}$$

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 (5.2), it is denoted by $\rho^n(s)$. Let $P^n(s)$ denote the set of hypothesis-unaware policies with memory over an n-slot time horizon and satisfying (5.2), i.e., $\rho^n(s) \in P^n(s)$. 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

$$\beta_{\mathrm{M}}(n, \varepsilon, s) \triangleq \max_{\rho^n(s) \in P^n(s)} \{\beta(n, \varepsilon, \rho^n(s))\}. \tag{5.23}$$

Define a Kullback-Leibler divergence rate expression $\theta_{\mathrm{M}}(s)$ as

$$\theta_{\mathrm{M}}(s) \triangleq \inf_{k\in\mathbb{Z}_+}\left\{\inf_{\rho^k(s)\in P^k(s)}\left\{\frac{1}{k}\mathrm{D}(p_{Y^k|h_0}||p_{Y^k|h_1})\right\}\right\}. \tag{5.24}$$

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

Corollary 5.3. *Given $s > 0$,*

$$\lim_{\varepsilon\to 1}\lim_{n\to\infty}\frac{1}{n}\log\frac{1}{\beta_{\mathrm{M}}(n,\varepsilon,s)} = \theta_{\mathrm{M}}(s). \tag{5.25}$$

The privacy-preserving memoryless hypothesis-aware policy has access to the correct hypothesis without the information of the past demands and supplies while the privacy-preserving hypothesis-unaware policy with memory has the information of the past demands and supplies without the knowledge of the correct hypothesis. The asymptotic privacy-preserving performances of the two policies are compared in the following theorem.

Theorem 5.3. *Given $s > 0$,*

$$\theta_{\mathrm{M}}(s) \leq \phi(s,s). \tag{5.26}$$

The proof ideas of Theorem 5.3 are to construct a two-phase hypothesis-unaware policy with memory which first learns the hypothesis and to use its asymptotic privacy-preserving performance to relate $\theta_{\mathrm{M}}(s)$ with $\phi(s,s)$. The complete proof is presented in the appendix of this chapter.

Remark 5.3. *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 sequence.*

Asymptotic privacy-preserving guarantee

As shown in Corollaries 5.1-5.3, the asymptotic exponential decay rate of the maximum minimal Type II probability of error in the worst privacy leakage scenario can be characterized by a Kullback-Leibler 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,

the single-letter Kullback-Leibler divergence expression $\phi(s,s)$ can be used as an asymptotic privacy-preserving guarantee under the adversarial Neyman-Pearson hypothesis testing.

While solving the optimization problem in (5.18) 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. It is shown in the following 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 5.4. *The energy supply alphabet can be limited to the energy demand alphabet under both hypotheses without loss of optimality for the evaluation of* $\phi(s,s)$.

Proof. Suppose that $\phi(s,s) = \mathrm{D}(p^*_{Y|h_0}||p^*_{Y|h_1})$ is achieved by $p^*_{Y|X,h_0}$ and $p^*_{Y|X,h_1}$. Let $\mathcal{X} = \{x_{(1)}, \ldots, x_{(||\mathcal{X}||)}\}$ with $x_{(i)} < x_{(k)}$ if $i < k$. Consider the following quantization operation which maps y to $\hat{y}$:

$$\hat{y} = \begin{cases} x_{(i)}, & \text{if } y \in (x_{(i-1)}, x_{(i)}],\ i \geq 2 \\ x_{(1)}, & \text{if } y \in [0, x_{(1)}] \end{cases}.$$

It can be verified that $p_{\hat{Y}|X,h_0}$, $p_{\hat{Y}|X,h_1}$ satisfy the instantaneous and single-slot average energy constraints. From the optimality in the definition of $\phi(s,s)$, it follows

$$\phi(s,s) = \mathrm{D}(p^*_{Y|h_0}||p^*_{Y|h_1}) \leq \mathrm{D}(p_{\hat{Y}|h_0}||p_{\hat{Y}|h_1}).$$

In addition, due to the data processing inequality of Kullback-Leibler divergence [58, Theorem 9], it follows that

$$\phi(s,s) = \mathrm{D}(p^*_{Y|h_0}||p^*_{Y|h_1}) \geq \mathrm{D}(p_{\hat{Y}|h_0}||p_{\hat{Y}|h_1}).$$

Therefore,

$$\phi(s,s) = \mathrm{D}(p_{\hat{Y}|h_0}||p_{\hat{Y}|h_1}),$$

and the energy supply alphabet under both hypotheses can be constrained to $\mathcal{X}$ without loss of optimality. □

5.3 Adversarial Bayesian Hypothesis Testing

In this section, an adversarial Bayesian hypothesis test is considered for the informed AD. A particular Bayesian risk used here is the error probability of the AD. Thus, the minimal error probability of the AD measures the smart meter privacy leakage. For the adversarial Bayesian hypothesis testing model of smart meter privacy problem, the corresponding asymptotic privacy-preserving performance is studied.

Under the Bayesian hypothesis testing model, the informed AD is assumed to use the optimal hypothesis testing strategy to achieve the minimal error probability as

$$\alpha(n,\gamma^n(s)) \triangleq \min_{\mathcal{A}_n\subseteq\mathcal{Y}^n} \left\{p_0\cdot p_{Y^n|h_0}(\mathcal{A}_n^c)+p_1\cdot p_{Y^n|h_1}(\mathcal{A}_n)\right\},$$

where $\mathcal{A}_n$ and $\mathcal{A}_n^c$ denote the decision regions for h_0 and h_1 of the AD. Correspondingly, following the privacy-preserving objective, the EMU uses the optimal energy management policy which maximizes the minimal error probability of the AD as

$$\alpha(n,s) \triangleq \max_{\gamma^n(s)\in\Gamma^n(s)} \left\{\alpha(n,\gamma^n(s))\right\}. \tag{5.27}$$

The following study on the optimal privacy-preserving performance focuses on the asymptotic exponential decay rate of the maximum minimal error probability.

To this end, Chernoff information is introduced first. The Chernoff information of a probability distribution $P(Z)$ from another distribution $Q(Z)$ is defined as

$$\mathrm{C}(P(Z),Q(Z)) \triangleq \max_{0\le\tau\le 1} \left\{\mathrm{C}_\tau(P(Z),Q(Z))\right\},$$

where $\mathrm{C}_\tau(P(Z),Q(Z))$ is defined as

$$\mathrm{C}_\tau(P(Z),Q(Z)) \triangleq -\log\left(\sum_{z\in\mathcal{Z}} P^\tau(z)Q^{1-\tau}(z)\right).$$

The convexity of Chernoff information is shown in the following propositions[1].

Proposition 5.1. *Given $0\le\tau\le 1$, the function $\mathrm{C}_\tau(P(Z),Q(Z))$ is jointly convex in $P(Z)$ and $Q(Z)$.*

Proof. Given $0\le\tau<1$, the function $\mathrm{C}_\tau(P(Z),Q(Z))$ is related to the Rényi divergence $\mathrm{D}_\tau(P(Z)||Q(Z))$ as

$$\mathrm{C}_\tau(P(Z),Q(Z)) = (1-\tau)\cdot\mathrm{D}_\tau(P(Z)||Q(Z)).$$

The convexity of $\mathrm{C}_\tau(P(Z),Q(Z))$ follows from the convexity of Rényi divergence [58, Theorem 11] and the positive scaler $1-\tau$.

If $\tau=1$,

$$\mathrm{C}_1(P(Z),Q(Z)) = -\log\left(P\left(\{z\in\mathcal{Z}|Q(z)>0\}\right)\right) = \mathrm{D}_0(Q(Z)||P(Z)).$$

In this case, the convexity of $\mathrm{C}_1(P(Z),Q(Z))$ follows from the convexity of the 0-th order Rényi divergence. □

Proposition 5.2. *The Chernoff information $\mathrm{C}(P(Z),Q(Z))$ is jointly convex in $P(Z)$ and $Q(Z)$.*

[1]These results most likely have been shown somewhere before. Unfortunately, I did not find these literatures.

The convexity of $\mathrm{C}(P(Z), Q(Z))$ follows from the convexity of $\mathrm{C}_\tau(P(Z), Q(Z))$ for all $0 \leq \tau \leq 1$ and the conclusion that pointwise maximum preserves the convexity [8, Section 3.2.3].

Then, define a Chernoff information rate expression $\mu(s)$ as

$$\mu(s) \triangleq \inf_{k\in\mathbb{Z}_+} \left\{ \inf_{\gamma^k(s)\in\Gamma^k(s)} \left\{ \frac{1}{k} \mathrm{C}(p_{Y^k|h_0}, p_{Y^k|h_1}) \right\} \right\}. \tag{5.28}$$

The operational meaning of $\mu(s)$ is shown later. Similar to the Kullback-Leibler divergence rate $\theta(s)$, the infimum over k in the definition of the Chernoff information rate $\mu(s)$ is taken at the limit $k \to \infty$, as shown in the following lemma.

Lemma 5.3.

$$\mu(s) = \lim_{k\to\infty} \inf_{\gamma^k(s)\in\Gamma^k(s)} \left\{ \frac{1}{k} \mathrm{C}(p_{Y^k|h_0}, p_{Y^k|h_1}) \right\}.$$

Proof. Given any n, $l \in \mathbb{Z}_+$, as defined before, $(\gamma^n(s), \gamma^l(s))$ is an energy management policy satisfying the average energy constraint over an $(n+l)$-slot time horizon.

$$\begin{aligned}
&\inf_{\gamma^{n+l}(s)\in\Gamma^{n+l}(s)} \left\{ \mathrm{C}(p_{Y^{n+l}|h_0}, p_{Y^{n+l}|h_1}) \right\} \\
\leq\ &\inf_{(\gamma^n(s),\gamma^l(s))\in\Gamma^n(s)\times\Gamma^l(s)} \left\{ \mathrm{C}(p_{Y^{n+l}|h_0}, p_{Y^{n+l}|h_1}) \right\} \\
\overset{(a)}{=}\ &\inf_{(\gamma^n(s),\gamma^l(s))\in\Gamma^n(s)\times\Gamma^l(s)} \left\{ \max_{0\leq\tau\leq 1} \left\{ \mathrm{C}_\tau(p_{Y^n|h_0}, p_{Y^n|h_1}) + \mathrm{C}_\tau(p_{Y^l|h_0}, p_{Y^l|h_1}) \right\} \right\} \\
\leq\ &\inf_{(\gamma^n(s),\gamma^l(s))\in\Gamma^n(s)\times\Gamma^l(s)} \left\{ \max_{0\leq\kappa\leq 1} \left\{ \mathrm{C}_\kappa(p_{Y^n|h_0}, p_{Y^n|h_1}) \right\} + \max_{0\leq\sigma\leq 1} \left\{ \mathrm{C}_\sigma(p_{Y^l|h_0}, p_{Y^l|h_1}) \right\} \right\} \\
=\ &\inf_{\gamma^n(s)\in\Gamma^n(s)} \left\{ \mathrm{C}(p_{Y^n|h_0}, p_{Y^n|h_1}) \right\} + \inf_{\gamma^l(s)\in\Gamma^l(s)} \left\{ \mathrm{C}(p_{Y^l|h_0}, p_{Y^l|h_1}) \right\},
\end{aligned}$$

where (a) follows from the independence property $p_{Y^{n+l}|h_j} = p_{Y^n|h_j} \cdot p_{Y^l|h_j}$ for $j = 0, 1$ satisfied by the energy management policy $(\gamma^n(s), \gamma^l(s))$. Therefore, the sequence of $\inf_{\gamma^k(s)\in\Gamma^k(s)} \left\{ \mathrm{C}(p_{Y^k|h_0}, p_{Y^k|h_1}) \right\}$ is *subadditive*. Then, Lemma 5.3 follows from Fekete's lemma. □

The operational meaning of the Chernoff information rate $\mu(s)$ is shown in the following theorem that the asymptotic exponential decay rate of the maximum minimal error probability is characterized by $\mu(s)$.

Theorem 5.5. *Given $s > 0$,*

$$\lim_{n\to\infty} \frac{1}{n} \log \frac{1}{\alpha(n, s)} = \mu(s). \tag{5.29}$$

Proof. Given any $k \in \mathbb{Z}_+$, $\gamma^k(s)$, and the resulting $p_{Y^k|h_0}$, $p_{Y^k|h_1}$, as defined before, $\gamma^{kl}(s)$ is an energy management policy which repeatedly uses $\gamma^k(s)$ for l times and satisfies the average energy constraint over a kl-slot time horizon. From the optimality in the definition (5.27) and the theorem [12, Theorem 11.9.1], it follows that

$$\limsup_{l\to\infty} \frac{1}{kl} \log \frac{1}{\alpha(kl,s)} \leq \lim_{l\to\infty} \frac{1}{kl} \log \frac{1}{\alpha(kl,\gamma^{kl}(s))} = \frac{1}{k} \mathrm{C}(p_{Y^k|h_0}, p_{Y^k|h_1}).$$

For $k(l-1) < n \leq kl$, the following inequality holds as

$$\alpha(kl,s) \leq \alpha(n,s) \leq \alpha(k(l-1),s).$$

It follows that

$$\begin{aligned}
\limsup_{n\to\infty} \frac{1}{n} \log \frac{1}{\alpha(n,s)} &\leq \limsup_{l\to\infty} \frac{kl}{k(l-1)} \frac{1}{kl} \log \frac{1}{\alpha(kl,s)} \\
&= \limsup_{l\to\infty} \frac{1}{kl} \log \frac{1}{\alpha(kl,s)} \\
&\leq \frac{1}{k} \mathrm{C}(p_{Y^k|h_0}, p_{Y^k|h_1}),
\end{aligned}$$

for all $k \in \mathbb{Z}_+$ and $\gamma^k(s)$. Therefore, $\mu(s)$ is an upper bound on the asymptotic exponential decay rate of the maximum minimal error probability:

$$\limsup_{n\to\infty} \frac{1}{n} \log \frac{1}{\alpha(n,s)} \leq \mu(s). \tag{5.30}$$

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 $\alpha(n,s)$. An optimal hypothesis testing strategy of the AD is a deterministic LRT [59] with

$$\mathcal{A}^*_n = \left\{ y^n \left| \frac{p^*_{Y^n|h_0}(y^n)}{p^*_{Y^n|h_1}(y^n)} \geq \frac{p_1}{p_0} \right. \right\}.$$

Based on the optimal deterministic LRT of the AD, the maximum minimal error probability $\alpha(n,s)$ is equivalently expressed and upper bounds on it are derived as follows. For all $0 \leq \tau \leq 1$,

$$\begin{aligned}
\alpha(n,s) &= \sum_{y^n \in \mathcal{Y}^n} \min\left\{ p_0 \cdot p^*_{Y^n|h_0}(y^n), p_1 \cdot p^*_{Y^n|h_1}(y^n) \right\} \\
&\leq \sum_{y^n \in \mathcal{Y}^n} p_0^{\tau} \cdot p^{*\tau}_{Y^n|h_0}(y^n) \cdot p_1^{1-\tau} \cdot p^{*1-\tau}_{Y^n|h_1}(y^n) \\
&\leq \sum_{y^n \in \mathcal{Y}^n} p^{*\tau}_{Y^n|h_0}(y^n) p^{*1-\tau}_{Y^n|h_1}(y^n).
\end{aligned}$$

Therefore,

$$\begin{aligned}\frac{1}{n}\log\frac{1}{\alpha(n,s)} &\geq \frac{1}{n}\max_{0\leq\tau\leq 1}\left\{-\log\left(\sum_{y^n\in\mathcal{Y}^n} p^{*\tau}_{Y^n|h_0}(y^n)p^{*1-\tau}_{Y^n|h_1}(y^n)\right)\right\}\\ &= \frac{1}{n}\mathrm{C}(p^*_{Y^n|h_0}, p^*_{Y^n|h_1})\\ &\geq \inf_{\gamma^n(s)\in\Gamma^n(s)}\left\{\frac{1}{n}\mathrm{C}(p_{Y^n|h_0}, p_{Y^n|h_1})\right\}.\end{aligned}$$

In the asymptotic regime as $n\to\infty$, it follows that

$$\liminf_{n\to\infty}\frac{1}{n}\log\frac{1}{\alpha(n,s)} \geq \lim_{n\to\infty}\inf_{\gamma^n(s)\in\Gamma^n(s)}\left\{\frac{1}{n}\mathrm{C}(p_{Y^n|h_0}, p_{Y^n|h_1})\right\} = \mu(s), \tag{5.31}$$

where the final equality follows from Lemma 5.3.

The inequalities (5.30) and (5.31) jointly lead to Theorem 5.5. □

Over a finite time horizon, the prior distribution of the hypothesis determines the test threshold of the optimal LRT of the AD, and further determines the exponential decay rate of the maximum minimal error probability. However, as shown in Theorem 5.5, it is not the same when evaluating the asymptotic exponential decay rate of the maximum minimal error probability over an infinite time horizon.

Remark 5.4. *The asymptotic exponential decay rate of the maximum minimal error probability does not depend on the prior probability distribution of the binary hypothesis.*

In the following, the asymptotic optimal privacy-preserving performances of the memoryless hypothesis-aware policy and the hypothesis-unaware policy with memory are characterized under the adversarial Bayesian hypothesis testing.

Memoryless hypothesis-aware policy

When the EMU uses the optimal privacy-preserving memoryless hypothesis-aware policy under the adversarial Bayesian hypothesis testing, the achieved maximum minimal error probability is denoted by

$$\alpha_{\mathrm{L}}(n,s) \triangleq \max_{\pi^n(s)\in\Pi^n(s)}\{\alpha(n,\pi^n(s))\}. \tag{5.32}$$

Define a Chernoff information rate $\mu_{\mathrm{L}}(s)$ similar to $\mu(s)$ as

$$\mu_{\mathrm{L}}(s) \triangleq \inf_{k\in\mathbb{Z}_+}\left\{\inf_{\pi^k(s)\in\Pi^k(s)}\left\{\frac{1}{k}\mathrm{C}(p_{Y^k|h_0}, p_{Y^k|h_1})\right\}\right\}. \tag{5.33}$$

Following the proof of Theorem 5.5, it can be similarly shown that the asymptotic exponential decay rate of the maximum minimal error probability is specified by the Chernoff information rate expression $\mu_{\mathrm{L}}(s)$ when the EMU uses the optimal privacy-preserving memoryless hypothesis-aware policy.

Corollary 5.4. *Given $s > 0$,*

$$\lim_{n\to\infty} \frac{1}{n} \log \frac{1}{\alpha_{\mathrm{L}}(n,s)} = \mu_{\mathrm{L}}(s). \tag{5.34}$$

The two single-letter expressions defined in the following will be used to characterize upper and lower bounds on the asymptotic exponential decay rate of the maximum minimal error probability (or equivalently the Chernoff information rate $\mu_{\mathrm{L}}(s)$).

Given $\bar{s}$, $\tilde{s} > 0$ and $0 \leq \tau \leq 1$, define $\nu_\tau(\bar{s}, \tilde{s})$ as

$$\nu_\tau(\bar{s}, \tilde{s}) \triangleq \min_{(p_{Y|X,h_0}, p_{Y|X,h_1}) \in \mathcal{P}(\bar{s},\tilde{s})} \left\{ \mathrm{C}_\tau(p_{Y|h_0}, p_{Y|h_1}) \right\}; \tag{5.35}$$

and define a single-letter Chernoff information $\nu(\bar{s}, \tilde{s})$ as

$$\nu(\bar{s}, \tilde{s}) \triangleq \min_{(p_{Y|X,h_0}, p_{Y|X,h_1}) \in \mathcal{P}(\bar{s},\tilde{s})} \left\{ \mathrm{C}(p_{Y|h_0}, p_{Y|h_1}) \right\}. \tag{5.36}$$

Lemma 5.4. *For any $0 \leq \tau \leq 1$, $\nu_\tau(\bar{s}, \tilde{s})$ is a non-increasing and jointly convex function for $\bar{s} > 0$ and $\tilde{s} > 0$.*

Lemma 5.5. *$\nu(\bar{s}, \tilde{s})$ is a non-increasing, continuous, and jointly convex function for $\bar{s} > 0$ and $\tilde{s} > 0$.*

The proofs of Lemmas 5.4 and 5.5 use the same arguments as the proof of Lemma 5.2 and are therefore omitted.

Lemma 5.6. *Given $s > 0$, the Chernoff information rate $\mu_{\mathrm{L}}(s)$ has single-letter upper and lower bounds as*

$$\max_{0\leq\tau\leq 1} \{\nu_\tau(s,s)\} \leq \mu_{\mathrm{L}}(s) \leq \nu(s,s). \tag{5.37}$$

Proof. For any $0 \leq \tau \leq 1$, $k \in \mathbb{Z}_+$, $\pi^k(s)$, and the resulting $p_{Y^k|h_0}$, $p_{Y^k|h_1}$, the

Chernoff information rate $\frac{1}{k}\mathrm{C}(p_{Y^k|h_0}, p_{Y^k|h_1})$ is lower bounded by $\nu_\tau(s,s)$ as

$$\begin{aligned}
&\frac{1}{k}\mathrm{C}(p_{Y^k|h_0}, p_{Y^k|h_1}) \\
&= \frac{1}{k}\max_{0\le\kappa\le 1}\left\{\mathrm{C}_\kappa\left(p_{Y^k|h_0}, p_{Y^k|h_1}\right)\right\} \\
&\ge \frac{1}{k}\mathrm{C}_\tau\left(p_{Y^k|h_0}, p_{Y^k|h_1}\right) \\
&\overset{(a)}{=} \frac{1}{k}\sum_{i=1}^{k}\mathrm{C}_\tau\left(p_{Y_i|h_0}, p_{Y_i|h_1}\right) \\
&\overset{(b)}{\ge} \frac{1}{k}\sum_{i=1}^{k}\nu_\tau\left(\mathrm{E}[X_i - Y_i|h_0], \mathrm{E}[X_i - Y_i|h_1]\right) \\
&\overset{(c)}{\ge} \nu_\tau\left(\mathrm{E}\left[\frac{1}{k}\sum_{i=1}^{k}(X_i - Y_i|h_0)\right], \mathrm{E}\left[\frac{1}{k}\sum_{i=1}^{k}(X_i - Y_i|h_1)\right]\right) \\
&\overset{(d)}{\ge} \nu_\tau(s,s),
\end{aligned} \tag{5.38}$$

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 $\nu_\tau(\bar{s}, \tilde{s})$; (c) follows from the convexity of $\nu_\tau(\bar{s}, \tilde{s})$; and (d) follows from the non-increasing property of $\nu_\tau(\bar{s}, \tilde{s})$.

Thus, for any $k \in \mathbb{Z}_+$, $\pi^k(s)$, and the resulting $p_{Y^k|h_0}$, $p_{Y^k|h_1}$, the following inequality holds as

$$\frac{1}{k}\mathrm{C}(p_{Y^k|h_0}, p_{Y^k|h_1}) \ge \max_{0\le\tau\le 1}\left\{\nu_\tau(s,s)\right\},$$

since (5.38) holds for all $0 \le \tau \le 1$. It further follows that

$$\mu_{\mathrm{L}}(s) = \inf_{k\in\mathbb{Z}_+}\left\{\inf_{\pi^k(s)\in\Pi^k(s)}\left\{\frac{1}{k}\mathrm{C}(p_{Y^k|h_0}, p_{Y^k|h_1})\right\}\right\} \ge \max_{0\le\tau\le 1}\left\{\nu_\tau(s,s)\right\}.$$

The other inequality $\mu_{\mathrm{L}}(s) \le \nu(s,s)$ in (5.37) follows from the definitions of $\mu_{\mathrm{L}}(s)$ and $\nu(s,s)$. □

Under the adversarial Bayesian hypothesis testing and using the memoryless hypothesis-aware policy, a max min single-letter lower bound and a min max single-letter upper bound on the asymptotic exponential decay rate of the maximum minimal error probability are obtained. In the following theorem, it is shown that the two bounds are equal and the asymptotic exponential decay rate of the maximum minimal error probability can be specified by the single-letter Chernoff information $\nu(s,s)$.

Theorem 5.6. *Given $s > 0$,*

$$\mu_{\mathrm{L}}(s) = \nu(s,s). \tag{5.39}$$

Proof. Given $s > 0$, the lower and upper bounds shown in Lemma 5.6 can be specified by a max min expression and a min max expression as

$$\max_{0\leq\tau\leq 1}\{\nu_\tau(s,s)\} = \max_{0\leq\tau\leq 1}\left\{\min_{(p_{Y|X,h_0},p_{Y|X,h_1})\in\mathcal{P}(s,s)}\left\{\mathrm{C}_\tau(p_{Y|h_0},p_{Y|h_1})\right\}\right\},$$
$$\nu(s,s) = \min_{(p_{Y|X,h_0},p_{Y|X,h_1})\in\mathcal{P}(s,s)}\left\{\max_{0\leq\tau\leq 1}\left\{\mathrm{C}_\tau(p_{Y|h_0},p_{Y|h_1})\right\}\right\}.$$

If τ is fixed, $\mathrm{C}_\tau(p_{Y|h_0},p_{Y|h_1})$ is a jointly convex function in $p_{Y|X,h_0}$ and $p_{Y|X,h_1}$, which follows from the convexity of $\mathrm{C}_\tau(\cdot,\cdot)$ shown in Proposition 5.1 and the convexity-preserving composition rule in [8, Section 3.2.4]. If $p_{Y|X,h_0}$ and $p_{Y|X,h_1}$ are fixed, $p_{Y|h_0}$ and $p_{Y|h_1}$ are fixed, and $\mathrm{C}_\tau(p_{Y|h_0},p_{Y|h_1})$ is a concave function in τ, which follows from the result [58, Corollary 2].

From von Neumann's minimax theorem [49], it follows that

$$\max_{0\leq\tau\leq 1}\{\nu_\tau(s,s)\} = \nu(s,s). \tag{5.40}$$

Lemma 5.6 and (5.40) jointly lead to Theorem 5.6. □

Remark 5.5. *Given $s > 0$, the asymptotic exponential decay rate of the maximum minimal error probability $\lim_{n\to\infty}\frac{1}{n}\log\frac{1}{\alpha_{\mathrm{L}}(n,s)}$ can be achieved by a memoryless hypothesis-aware policy which uses the same single-slot policy $(p^*_{Y|X,h_0},p^*_{Y|X,h_1})$ corresponding to the optimizer of $\nu(s,s)$ at all time slots.*

Hypothesis-unaware policy with memory

In this section, hypothesis-unaware policy with memory, the "counter" case of memoryless hypothesis-aware policy, is considered. When the EMU uses the optimal privacy-preserving hypothesis-unaware policy with memory under the adversarial Bayesian hypothesis testing, the achieved maximum minimal error probability is denoted by

$$\alpha_{\mathrm{M}}(n,s) \triangleq \max_{\rho^n(s)\in P^n(s)}\{\alpha(n,\rho^n(s))\}. \tag{5.41}$$

Define a Chernoff information rate $\mu_{\mathrm{M}}(s)$ as

$$\mu_{\mathrm{M}}(s) \triangleq \inf_{k\in\mathbb{Z}_+}\left\{\inf_{\rho^k(s)\in P^k(s)}\left\{\frac{1}{k}\mathrm{C}\left(p_{Y^k|h_0},p_{Y^k|h_1}\right)\right\}\right\}, \tag{5.42}$$

which characterizes the asymptotic exponential decay rate of the maximum minimal error probability as shown in the following corollary.

Corollary 5.5. *Given $s > 0$,*

$$\lim_{n\to\infty} \frac{1}{n} \log \frac{1}{\alpha_{\mathrm{M}}(n, s)} = \mu_{\mathrm{M}}(s). \tag{5.43}$$

Under the adversarial Bayesian hypothesis testing, the following theorem compares the asymptotic privacy-preserving performances of the optimal memoryless hypothesis-aware policy and the optimal hypothesis-unaware policy with memory.

Theorem 5.7. *Given $s > 0$,*

$$\mu_{\mathrm{M}}(s) \leq \nu(s, s). \tag{5.44}$$

The proof idea of Theorem 5.7 is similar to that of Theorem 5.3 through constructing a two-phase hypothesis-unaware policy with memory which first learns the correct hypothesis, and using the asymptotic privacy-preserving performance of the constructed policy to relate $\mu_{\mathrm{M}}(s)$ with $\nu(s, s)$. The complete proof of Theorem 5.7 is presented in the appendix of this chapter.

Remark 5.6. *Under the adversarial Bayesian hypothesis testing and in the asymptotic regime, the optimal privacy-preserving memoryless hypothesis-aware policy cannot outperform the optimal privacy-preserving hypothesis-unaware policy with memory.*

Asymptotic privacy-preserving guarantee

As shown in Theorem 5.5, Corollaries 5.4 and 5.5, the asymptotic exponential decay rate of the maximum minimal error probability of the AD can be specified by a Chernoff information rate. Similarly, the numerical evaluation of $\mu(s)$ or $\mu_{\mathrm{M}}(s)$ is difficult. On the other hand, $\nu(s, s)$ provides an upper bound on the optimal asymptotic exponential decay rate. Hence, the single-letter Chernoff information $\nu(s, s)$ is used as an asymptotic privacy-preserving guarantee under the adversarial Bayesian hypothesis testing.

While solving the optimization problem in (5.36) leads to the asymptotic privacy-preserving guarantee, the energy supply alphabet $\mathcal{Y}$ can be arbitrarily large which means a highly complex optimization problem. The following theorem shows that the alphabet $\mathcal{Y}$ can be limited to the alphabet $\mathcal{X}$ which typically corresponds to a set of limited number of appliance operation modes. This result can greatly simplify the numerical evaluation of the asymptotic privacy-preserving guarantee.

Theorem 5.8. *The energy supply alphabet can be limited to the energy demand alphabet under both hypotheses without loss of optimality for the evaluation of $\nu(s, s)$.*

Proof. Suppose that $\nu(s,s) = \mathrm{C}(p^*_{Y|h_0}, p^*_{Y|h_1})$ is achieved by $p^*_{Y|X,h_0}$ and $p^*_{Y|X,h_1}$. Let $\mathcal{X} = \{x_{(1)}, \ldots, x_{(||\mathcal{X}||)}\}$ with $x_{(i)} < x_{(k)}$ if $i < k$. Consider the following quantization operation which maps y to $\hat{y}$:

$$\hat{y} = \begin{cases} x_{(i)}, & \text{if } y \in (x_{(i-1)}, x_{(i)}],\ i \geq 2 \\ x_{(1)}, & \text{if } y \in [0, x_{(1)}] \end{cases}.$$

It can be verified that $p_{\hat{Y}|X,h_0}$, $p_{\hat{Y}|X,h_1}$ satisfy the instantaneous and single-slot average energy constraints. From the optimality in the definition of $\nu(s,s)$, it follows

$$\nu(s,s) = \mathrm{C}(p^*_{Y|h_0}, p^*_{Y|h_1}) \leq \mathrm{C}(p_{\hat{Y}|h_0}, p_{\hat{Y}|h_1}).$$

In addition, from the data processing inequality of Rényi divergence [58, Theorem 9], it follows

$$\begin{aligned}
\nu(s,s) &= \mathrm{C}(p^*_{Y|h_0}, p^*_{Y|h_1}) \\
&= \max_{0\leq\tau\leq 1} \left\{ \mathrm{C}_\tau(p^*_{Y|h_0}, p^*_{Y|h_1}) \right\} \\
&= \max \left\{ \max_{0\leq\tau<1} \left\{ (1-\tau)\mathrm{D}_\tau(p^*_{Y|h_0}||p^*_{Y|h_1}) \right\}, \mathrm{D}_0(p^*_{Y|h_1}||p^*_{Y|h_0}) \right\} \\
&\geq \max \left\{ \max_{0\leq\tau<1} \left\{ (1-\tau)\mathrm{D}_\tau(p_{\hat{Y}|h_0}||p_{\hat{Y}|h_1}) \right\}, \mathrm{D}_0(p_{\hat{Y}|h_1}||p_{\hat{Y}|h_0}) \right\} \\
&= \max_{0\leq\tau\leq 1} \left\{ \mathrm{C}_\tau(p_{\hat{Y}|h_0}, p_{\hat{Y}|h_1}) \right\} \\
&= \mathrm{C}(p_{\hat{Y}|h_0}, p_{\hat{Y}|h_1}).
\end{aligned}$$

Therefore,

$$\nu(s,s) = \mathrm{C}(p_{\hat{Y}|h_0}, p_{\hat{Y}|h_1}),$$

and the energy supply alphabet under both hypotheses can be constrained to $\mathcal{X}$ without loss of optimality. □

5.4 Numerical Example

Binary demand

This example is with binary energy demands $\mathcal{X} = \{0, 2\}$. Based on Theorem 5.4 or Theorem 5.8, it is sufficient to consider the binary supply alphabet $\mathcal{Y} = \{0, 2\}$. Denote $p_{X|h_0}(0)$ by $\bar{p}$ and $p_{X|h_1}(0)$ by $\tilde{p}$.

Under the adversarial Neyman-Pearson test, the asymptotic privacy-preserving guarantee, $\phi(s,s)$, is shown in Figure 5.2 for different values of $\bar{p}$ and $\tilde{p}$. Confirming the claim in Lemma 5.2, it can be observed 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

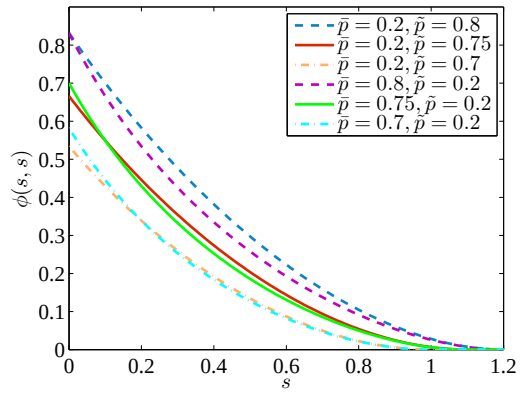


Figure 5.2: Asymptotic privacy-preserving guarantee $\phi(s, s)$ for a binary demand model under different settings of $\bar{p}$, $\tilde{p}$.

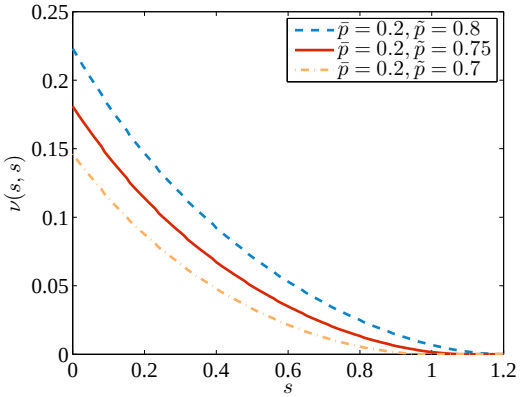


Figure 5.3: Asymptotic privacy-preserving guarantee $\nu(s, s)$ for a binary demand model under different settings of $\bar{p}$, $\tilde{p}$.

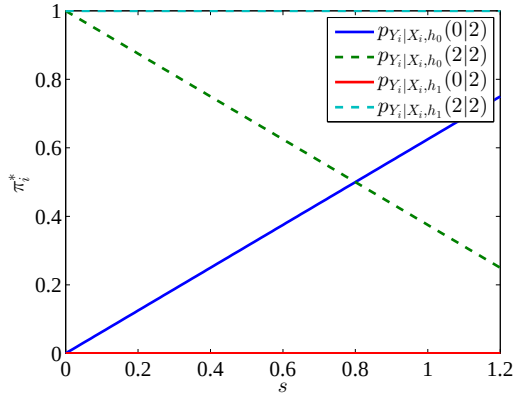


Figure 5.4: Asymptotically optimal memoryless hypothesis-aware instantaneous policy under the settings of $\bar{p} = 0.2$, $\tilde{p} = 0.8$.

more similar energy demand profiles. It can be observed in Figure 5.2 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 $(\bar{p}, \tilde{p})_{(\mathrm{B})}$.

Under the adversarial Bayesian hypothesis testing, the asymptotic privacy-preserving guarantee, $\nu(s, s)$, is shown in Figure 5.3 for different values of $\bar{p}$ and $\tilde{p}$. Confirming the claim in Lemma 5.5, the asymptotic privacy-preserving guarantee $\nu(s, s)$ is a convex and non-increasing function of s. From the same argument that more similar energy demand profiles make the AD more difficult to identify the hypotheses, it follows that $\nu(s, s)$ decreases as $\tilde{p}$ gets closer to the fixed $\bar{p}$. Note that the "opposite" settings, $(\bar{p} = 0.8, \tilde{p} = 0.2)$, $(\bar{p} = 0.75, \tilde{p} = 0.2)$, and $(\bar{p} = 0.7, \tilde{p} = 0.2)$, are not presented here since they lead to the same privacy-preserving guarantee curves as presented in the figure.

From the numerical result, the RES average energy generation rate needed to guarantee a certain privacy-preserving performance can be determined.

Figure 5.4 shows the asymptotically optimal memoryless hypothesis-aware instantaneous policy which achieves the privacy-preserving guarantees $\phi(s, s)$ and $\nu(s, s)$ under the settings of $\bar{p} = 0.2$ and $\tilde{p} = 0.8$. The instantaneous constraint has determined that $p_{Y_i|X_i,h_j}(0|0) = 1$ and $p_{Y_i|X_i,h_j}(2|0) = 0$ for all $j \in \{0, 1\}$. Note that it is generally not true to have a memoryless hypothesis-aware instantaneous policy which achieves both $\phi(s, s)$ and $\nu(s, s)$.

5.5 Summary

In this chapter, two adversarial hypothesis testings are considered for the smart meter privacy problem. The asymptotic privacy-preserving performances are characterized.

When the adversarial Neyman-Pearson hypothesis testing is considered, asymptotic optimal privacy-preserving performance can be characterized by a Kullback-Leibler divergence rate. In the worst case scenario where the Type I probability of error upper bound is close to one, a single-letter Kullback-Leibler divergence is obtained 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 the privacy-preserving memoryless hypothesis-aware policy is shown not to outperform the privacy-preserving hypothesis-unaware policy with memory since the EMU can learn the correct hypothesis through a sufficiently long energy demand sequence with an arbitrarily small probability of error. Without loss of optimality, the energy supply alphabet can be constrained to the energy demand alphabet for the evaluation of the single-letter-divergence privacy-preserving guarantee, which can simplify the problem and the numerical simulation. Furthermore, the construction of the optimal privacy-preserving memoryless hypothesis-aware policy is shown.

When the adversarial Bayesian hypothesis testing is considered and the privacy leakage is measured by the minimal error probability of the AD, similar results about the asymptotic optimal privacy-preserving performances are obtained as these for the adversarial Neyman-Pearson hypothesis testing by substituting Kullback-Leibler divergence with Chernoff information.

5.6 Appendix

Proof of Theorem 5.3

Proof. Let $o(n) \triangleq \lfloor \log n \rfloor$, $c(n) \triangleq \lfloor \log n \rfloor + 1$, and $q(n) \triangleq n - \lfloor \log n \rfloor$. Choose any $\delta \in (0, s)$, $\omega \in (0, s)$, and Type I probability of error upper bound $\varepsilon' \in (\max\{0, 1 - \min\{\mathrm{D}(p_{X|h_0}||p_{X|h_1}), \frac{\delta}{\max \mathcal{X}}\}\}, 1)$. Then set $\xi = 1 - \varepsilon'$ and $\psi = \delta - \max \mathcal{X} \cdot \xi$. It can be verified that $0 < \xi < \mathrm{D}(p_{X|h_0}||p_{X|h_1})$ and $0 < \psi \leq \delta$. These parameters are used to construct a hypothesis-unaware energy management policy with memory ρ_{p}^n over an n-slot time horizon, which consists of two successive phases.

$o(n)$-slot learning phase. The goal of the EMU is to learn the correct hypothesis at the end of the first phase. To prevent privacy leakage during the learning phase, identical instantaneous energy management policies are used at all time slots as:

$$y_i = \rho_i(x_i) = \min \mathcal{X},\ \forall i \leq o(n),\ \forall x_i \in \mathcal{X}.$$

Based on the observations of energy demands $x^{o(n)}$, the EMU makes a decision $\hat{H}$:

$$\hat{H} = \begin{cases} h_0, \text{ if } x^{o(n)} \in \mathcal{A}_\xi^{o(n)}(p_{X|h_0}||p_{X|h_1}) \\ h_1, \text{ otherwise} \end{cases},$$

where $\mathcal{A}_\xi^{o(n)}(p_{X|h_0}||p_{X|h_1})$ denotes a relative entropy typical set as defined in [12] and any sequence $x^{o(n)} \in \mathcal{A}_\xi^{o(n)}(p_{X|h_0}||p_{X|h_1})$ satisfies

$$\left| \frac{1}{o(n)} \log \frac{p_{X^{o(n)}|h_0}\left(x^{o(n)}\right)}{p_{X^{o(n)}|h_1}\left(x^{o(n)}\right)} - \mathrm{D}(p_{X|h_0}||p_{X|h_1}) \right| \leq \xi.$$

The EMU can make a wrong decision. Let $p_{\bar{e}} = 1 - p_{X^{o(n)}|h_0}(\mathcal{A}_\xi^{o(n)}(p_{X|h_0}||p_{X|h_1}))$ denote the Type I probability of error and $p_{\tilde{e}} = p_{X^{o(n)}|h_1}(\mathcal{A}_\xi^{o(n)}(p_{X|h_0}||p_{X|h_1}))$ denote the Type II probability of error for the EMU.

$q(n)$-slot privacy-preserving phase. Depending on the decision $\hat{H}$ in the learning phase, identical instantaneous energy management policies are used at all slots of the second phase as follows.
If $\hat{H} = h_0$ (resp. $\hat{H} = h_1$) and for all $i \in \{c(n), \ldots, n\}$, ρ_i corresponds to the optimizer $p^*_{Y|X,h_0}$ (resp. $p^*_{Y|X,h_1}$) of $\phi(s - \delta, s - \omega)$.

The instantaneous constraint is always satisfied by the proposed energy management policy ρ_{p}^n. Next, the average energy constraint is checked. Under hypothesis h_0 (resp. h_1), if a correct learning is achieved, the instantaneous energy management policies used in the privacy-preserving phase guarantee that the single-slot average energy upper bound $s - \delta$ (resp. $s - \omega$) is satisfied at all time slots of this phase; otherwise, bounded violation of the single-slot average energy constraint might happen at all time slots of the privacy-preserving phase. When n is suffi-

ciently large,

$$
\begin{aligned}
&\mathrm{E}\left[\frac{1}{n}\sum_{i=1}^{n}(X_i - Y_i)\middle| h_0\right] \\
&\leq \frac{o(n)}{n}\max\mathcal{X} + \mathrm{E}\left[\frac{1}{n}\sum_{i=c(n)}^{n}(X_i - Y_i)\middle| h_0\right] \\
&= \frac{o(n)}{n}\max\mathcal{X} + \mathrm{E}\left[\frac{1}{n}\sum_{i=c(n)}^{n}(X_i - Y_i)\middle| \hat{H} = h_1, H = h_0\right] p_{\bar{e}} \\
&\quad + \mathrm{E}\left[\frac{1}{n}\sum_{i=c(n)}^{n}(X_i - Y_i)\middle| \hat{H} = h_0, H = h_0\right](1 - p_{\bar{e}}) \\
&\overset{(a)}{\leq} \frac{o(n)}{n}\max\mathcal{X} + \frac{q(n)}{n}(s - \delta + \max\mathcal{X}\cdot\xi) \\
&\leq s - \delta + \max\mathcal{X}\cdot\xi + \frac{o(n)}{n}\max\mathcal{X} \\
&= s - (\psi - \frac{o(n)}{n}\max\mathcal{X}) \\
&\overset{(b)}{\leq} s,
\end{aligned}
$$

and

$$
\begin{aligned}
&\mathrm{E}\left[\frac{1}{n}\sum_{i=1}^{n}(X_i - Y_i)\middle| h_1\right] \\
&\leq \frac{o(n)}{n}\max\mathcal{X} + \mathrm{E}\left[\frac{1}{n}\sum_{i=c(n)}^{n}(X_i - Y_i)\middle| h_1\right] \\
&= \frac{o(n)}{n}\max\mathcal{X} + \mathrm{E}\left[\frac{1}{n}\sum_{i=c(n)}^{n}(X_i - Y_i)\middle| \hat{H} = h_0, H = h_1\right] p_{\bar{e}} \\
&\quad + \mathrm{E}\left[\frac{1}{n}\sum_{i=c(n)}^{n}(X_i - Y_i)\middle| \hat{H} = h_1, H = h_1\right](1 - p_{\bar{e}}) \\
&\leq \frac{o(n)}{n}\max\mathcal{X} + \frac{q(n)}{n}(s - \omega + \max\mathcal{X}\cdot p_{\bar{e}}) \\
&\overset{(c)}{\leq} s + \underbrace{\max\mathcal{X}\cdot e^{-o(n)\cdot(\mathrm{D}(p_{X|h_0}||p_{X|h_1})-\xi)} + \frac{o(n)}{n}\max\mathcal{X} - \omega}_{\Delta(n)} \\
&\overset{(d)}{\leq} s,
\end{aligned}
$$

where (a) follows since $p_{\bar{e}} < \xi$ when $o(n)$ is sufficiently large [12, Theorem 11.8.2]; (b) follows since $\psi - \frac{o(n)}{n} \max \mathcal{X} \geq 0$ when n is sufficiently large; (c) follows since $p_{\tilde{e}} < e^{-o(n)\cdot(\mathrm{D}(p_{X|h_0}||p_{X|h_1})-\xi)}$ [12, Theorem 11.8.2]; and (d) follows since $\Delta(n) \leq 0$ when n is sufficiently large.

Therefore, ρ_{p}^n is an energy management policy which satisfies the average energy constraint in (5.2) when n is sufficiently large. Then, it follows that

$$\liminf_{n\to\infty} \frac{1}{q(n)} \log \frac{1}{\beta(n,\varepsilon',\rho_{\mathrm{p}}^n)} \geq \liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta(n,\varepsilon',\rho_{\mathrm{p}}^n)} \geq \liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta_{\mathrm{M}}(n,\varepsilon',s)}, \tag{5.45}$$

where the first inequality follows from $q(n) \leq n$; and the second inequality follows since the constructed energy management policy ρ_{p}^n is not necessarily optimal for all sufficiently large n.

From the point of view of the informed AD, the observations $y^{o(n)}$ in the learning phase do not reveal any information about the hypothesis. Therefore, the strategy of the AD only depends on the observation statistics in the privacy-preserving phase $p_{Y^n_{c(n)}|h_0}$ and $p_{Y^n_{c(n)}|h_1}$. Then, the term $\frac{1}{q(n)} \log \frac{1}{\beta(n,\varepsilon',\rho_{\mathrm{p}}^n)}$ in (5.45) represents the exponential decay rate of the minimal Type II probability of error in the privacy-preserving phase. With the energy management policy ρ_{p}^n specified above, the energy supply sequence in the privacy-preserving phase is a mixture of the i.i.d. sequences $Y^n_{c(n)}|\hat{H}=h_0, H=h_0$ and $Y^n_{c(n)}|\hat{H}=h_1, H=h_0$ under hypothesis h_0, or a mixture of the i.i.d. sequences $Y^n_{c(n)}|\hat{H}=h_1, H=h_1$ and $Y^n_{c(n)}|\hat{H}=h_0, H=h_1$ under hypothesis h_1. The probability distributions are

$$\begin{aligned} p_{Y^n_{c(n)}|h_0}\left(y^n_{c(n)}\right) &= (1-p_{\bar{e}}) \cdot p_{Y^n_{c(n)}|\hat{H}=h_0,H=h_0}\left(y^n_{c(n)}\right) \\ &\quad + p_{\bar{e}} \cdot p_{Y^n_{c(n)}|\hat{H}=h_1,H=h_0}\left(y^n_{c(n)}\right), \\ p_{Y^n_{c(n)}|h_1}\left(y^n_{c(n)}\right) &= (1-p_{\bar{e}}) \cdot p_{Y^n_{c(n)}|\hat{H}=h_1,H=h_1}\left(y^n_{c(n)}\right) \\ &\quad + p_{\tilde{e}} \cdot p_{Y^n_{c(n)}|\hat{H}=h_0,H=h_1}\left(y^n_{c(n)}\right). \end{aligned}$$

Define

$$\mathcal{B}(R,n) \triangleq \left\{ y^n_{c(n)} \left| \frac{1}{q(n)} \log \frac{p_{Y^n_{c(n)}|h_0}\left(y^n_{c(n)}\right)}{p_{Y^n_{c(n)}|h_1}\left(y^n_{c(n)}\right)} \leq R \right. \right\},$$

and

$$K(R) \triangleq \limsup_{n\to\infty} p_{Y^n_{c(n)}|h_0}\left(\mathcal{B}(R,n)\right).$$

From the information-spectrum results [10, Theorem 1], [19, Theorem 4.2.1], it follows that

$$\sup\{R|K(R) \leq \varepsilon'\} \geq \liminf_{n\to\infty} \frac{1}{q(n)} \log \frac{1}{\beta(n,\varepsilon',\rho_{\mathrm{p}}^n)}. \tag{5.46}$$

In the asymptotic regime as $n \to \infty$, $Y_{c(n)}^n|h_1$ can be seen as the i.i.d. sequence $Y_{c(n)}^n|\hat{H} = h_1, H = h_1$ since $\lim_{n\to\infty} p_{\bar{e}} \leq \lim_{n\to\infty} e^{-o(n)\cdot(\mathrm{D}(p_{X|h_0}||p_{X|h_1})-\xi)} = 0$. Based on the case study [19, Example 4.2.1], the upper bound $\sup\{R|K(R) \leq \varepsilon'\}$ is characterized by the divergences $\mathrm{D}_1 = \mathrm{D}(p_{Y|\hat{H}=h_0,H=h_0}||p_{Y|\hat{H}=h_1,H=h_1})$ and $\mathrm{D}_2 = \mathrm{D}(p_{Y|\hat{H}=h_1,H=h_0}||p_{Y|\hat{H}=h_1,H=h_1})$ as follows.
If $\mathrm{D}_1 \geq \mathrm{D}_2$,

$$\mathrm{D}(p_{Y|\hat{H}=h_0,H=h_0}||p_{Y|\hat{H}=h_1,H=h_1}) \geq \sup\{R|K(R) \leq \varepsilon'\};$$

otherwise, since $1 - p_{\bar{e}} > 1 - \xi = \varepsilon'$ as $n \to \infty$,

$$\mathrm{D}(p_{Y|\hat{H}=h_0,H=h_0}||p_{Y|\hat{H}=h_1,H=h_1}) = \sup\{R|K(R) \leq \varepsilon'\}.$$

Then, it follows that

$$\phi(s-\delta, s-\omega) = \mathrm{D}(p_{Y|\hat{H}=h_0,H=h_0}||p_{Y|\hat{H}=h_1,H=h_1}) \geq \sup\{R|K(R) \leq \varepsilon'\}. \quad (5.47)$$

The inequalities (5.45), (5.46), and (5.47) jointly lead to

$$\phi(s-\delta, s-\omega) \geq \liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta_{\mathrm{M}}(n, \varepsilon', s)}. \quad (5.48)$$

Given $\delta, \omega \in (0, s)$, the inequality (5.48) holds for all Type I probability of error upper bounds $\varepsilon' \in (\max\{0, 1 - \min\{\mathrm{D}(p_{X|h_0}||p_{X|h_1}), \frac{\delta}{\max \mathcal{X}}\}\}, 1)$. Therefore,

$$\phi(s-\delta, s-\omega) \geq \lim_{\varepsilon\to 1} \liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta_{\mathrm{M}}(n, \varepsilon, s)} = \theta_{\mathrm{M}}(s). \quad (5.49)$$

Since the inequality (5.49) holds for all $\delta, \omega \in (0, s)$, it follows that

$$\phi(s, s) = \inf_{\delta,\omega\in(0,s)} \{\phi(s-\delta, s-\omega)\} \geq \theta_{\mathrm{M}}(s),$$

where the equality follows from the non-increasing and continuous properties of $\phi(\bar{s}, \tilde{s})$. □

Proof of Theorem 5.7

Proof. Again, let $o(n) \triangleq \lfloor \log n \rfloor$, $c(n) \triangleq \lfloor \log n \rfloor + 1$, and $q(n) \triangleq n - \lfloor \log n \rfloor$. Choose any $\delta \in (0, s)$, $\omega \in (0, s)$, and $\xi \in \left(0, \min\left\{\mathrm{D}(p_{X|h_0}||p_{X|h_1}), \frac{\delta}{\max \mathcal{X}}\right\}\right)$. Then set $\psi = \delta - \max \mathcal{X} \cdot \xi$. It can be verified that $0 < \psi < \delta$. These parameters are used to construct a hypothesis-unaware energy management policy with memory ρ_{q}^n over an n-slot time horizon, which similarly has two phases as ρ_{p}^n.

$o(n)$-slot learning phase. This phase is the same as the learning phase of ρ_{p}^n: Identical instantaneous privacy-unaware policies are independently used at all slots and always require an energy supply sequence of $\min \mathcal{X}$ regardless of the

energy demand sequence; and the learning decision at the end of this phase is $\hat{H} = 0$ if the energy demand sequence $x^{o(n)}$ is in the relative entropy typical set $\mathcal{A}_{\xi}^{o(n)}\left(p_{X|h_0}||p_{X|h_1}\right)$ or is $\hat{H} = 1$ otherwise. For the EMU, denote the Type I probability of learning error by $p_{\bar{e}}$ and the Type II probability of learning error by $p_{\tilde{e}}$.

$q(n)$-slot privacy-preserving phase. Depending on the decision $\hat{H}$ in the learning phase, identical instantaneous energy management policies are used at all slots of the second phase as follows.
If $\hat{H} = h_0$ (resp. $\hat{H} = h_1$) and for all $i \in \{c(n), \ldots, n\}$, ρ_i corresponds to the optimizer $p^*_{Y|X,h_0}$ (resp. $p^*_{Y|X,h_1}$) of $\nu(s-\delta, s-\omega)$.

The instantaneous constraint is always satisfied by the constructed energy management policy ρ_{q}^n. It follows from the same analysis on ρ_{p}^n that the policy ρ_{q}^n satisfies the average energy constraint in (5.2) when n is sufficiently large. Similar to (5.45), the following inequality holds:

$$\liminf_{n\to\infty} \frac{1}{q(n)} \log \frac{1}{\alpha(n, \rho_{\mathrm{q}}^n)} \geq \liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\alpha(n, \rho_{\mathrm{q}}^n)} \geq \lim_{n\to\infty} \frac{1}{n} \log \frac{1}{\alpha_{\mathrm{M}}(n, s)} = \mu_{\mathrm{M}}(s). \tag{5.50}$$

Since $y^{o(n)}$ in the learning phase is a deterministic sequence of $\min \mathcal{X}$, the strategy of the AD only depends on the observation statistics in the privacy-preserving phase $p_{Y^n_{c(n)}|h_0}$ and $p_{Y^n_{c(n)}|h_1}$. Then, the term $\frac{1}{q(n)} \log \frac{1}{\alpha(n,\rho_{\mathrm{q}}^n)}$ in (5.50) represents the exponential decay rate of the minimal error probability in the privacy-preserving phase. With the energy management policy ρ_{q}^n specified above, the energy supply sequence in the privacy-preserving phase is a mixture of the i.i.d. sequences $Y^n_{c(n)}|\hat{H} = h_0, H = h_0$ with a probability $1 - p_{\bar{e}}$ and $Y^n_{c(n)}|\hat{H} = h_1, H = h_0$ with a probability $p_{\bar{e}}$ under hypothesis h_0, or a mixture of the i.i.d. sequences $Y^n_{c(n)}|\hat{H} = h_1, H = h_1$ with a probability $1 - p_{\tilde{e}}$ and $Y^n_{c(n)}|\hat{H} = h_0, H = h_1$ with a probability $p_{\tilde{e}}$ under hypothesis h_1. In the asymptotic regime as $n \to \infty$, $Y^n_{c(n)}|h_1$ can be seen as the i.i.d. sequence $Y^n_{c(n)}|\hat{H} = h_1, H = h_1$ since $\lim_{n\to\infty} p_{\tilde{e}} \leq \lim_{n\to\infty} e^{-o(n)\cdot(\mathrm{D}(p_{X|h_0}||p_{X|h_1})-\xi)} = 0$. Then, the asymptotic exponential decay rate of the minimal error probability in the second phase can be expressed as

$$\begin{aligned} \liminf_{n\to\infty} \frac{1}{q(n)} \log \frac{1}{\alpha(n, \rho_{\mathrm{q}}^n)} &= \mathrm{C}(p_{Y|\hat{H}=h_0,H=h_0}, p_{Y|\hat{H}=h_1,H=h_1}) + \Delta(\xi) \\ &= \nu(s-\delta, s-\omega) + \Delta(\xi), \end{aligned} \tag{5.51}$$

where $\nu(s-\delta, s-\omega)$ corresponds to the asymptotic exponential decay rate of the minimal error probability in the privacy-preserving phase if $p_{\bar{e}} = 0$; and the term $\Delta(\xi)$ denotes the asymptotic impact of the i.i.d. sequence $Y^n_{c(n)}|\hat{H} = h_1, H = h_0$ with a probability $p_{\bar{e}}$ under hypothesis h_0. The inequalities (5.50) and (5.51) jointly lead to

$$\mu_{\mathrm{M}}(s) \leq \nu(s-\delta, s-\omega) + \Delta(\xi). \tag{5.52}$$

Since $\limsup_{n\to\infty} p_{\bar{e}} \leq \xi$, the term $\Delta(\xi)$ satisfies

$$\lim_{\xi\to 0} \Delta(\xi) = 0. \tag{5.53}$$

Given $\delta,\ \omega \in (0, s)$, (5.52) holds for all $\xi \in \left(0, \min\left\{\mathrm{D}(p_{X|h_0}||p_{X|h_1}), \frac{\delta}{\max \mathcal{X}}\right\}\right)$. Therefore,

$$\mu_{\mathrm{M}}(s) \leq \nu(s-\delta, s-\omega) + \lim_{\xi\to 0} \Delta(\xi) = \nu(s-\delta, s-\omega). \tag{5.54}$$

Since the inequality (5.54) holds for all $\delta,\ \omega \in (0, s)$, it follows that

$$\mu_{\mathrm{M}}(s) \leq \inf_{\delta,\omega\in(0,s)} \{\nu(s-\delta, s-\omega)\} = \nu(s, s), \tag{5.55}$$

where the equality follows from the non-increasing and continuous properties of $\nu(\bar{s}, \tilde{s})$. □

Chapter 6

Smart Meter Privacy in the Presence of an Energy Storage

An additive noise can manipulate and hide the energy demand profile. A such noise can be a sequence of renewable energy supplies which has been discussed in the previous chapter under assumptions of i.i.d. energy demands and an ideal renewable energy source (RES) equipped with a sufficiently large energy storage (ES). In this chapter, charging/discharging energy flows of a finite-capacity ES are to be optimally managed to distort the meter readings and to suppress smart meter privacy leakage. Different from the problem in the previous chapter, the finite-capacity ES inherently introduces memory in the smart meter system, i.e., the current ES state depends on the previous ES state, energy demand, and energy supply. Other system memory sources are also allowed. A Bayesian hypothesis testing measure is used to assess the privacy leakage. The optimization of energy management policy is shown to be cast to a Markov decision process (MDP) problem framework so that one can employ the established design algorithms.

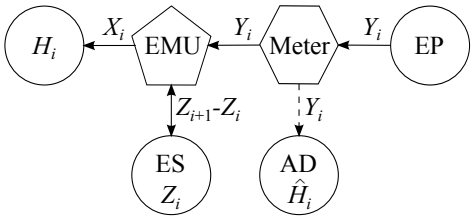


Figure 6.1: The smart meter privacy problem in the presence of a finite-capacity ES, where energy and information flows are represented by solid and dashed arrows, respectively.

6.1 System Model

As shown in Figure 6.1, the smart meter privacy problem is considered over an infinite time horizon. At every time slot $i \in \{1, 2, \dots\}$, denote the n-ary random consumer behavior hypothesis by H_i, the random energy demand of the consumer by X_i, the random ES state by Z_i, and the random energy supply from the EP by Y_i. W.l.o.g., consider the following finite non-negative integer alphabets: $\mathcal{H} = \{0, \dots, n-1\}$, $\mathcal{X} = \{0, \dots, u\}$, $\mathcal{Z} = \{0, \dots, m\}$, and $\mathcal{Y} = \{0, \dots, u+m\}$. Assume that the initial states (H_1, X_1, Z_1) are generated following the joint p.m.f. p_{H_1,X_1,Z_1}. The random hypothesis sequence H^∞ is assumed to be a first order Markov chain, i.e., H_i is generated depending on H_{i-1} only and following the time-invariant transition conditional p.m.f. $p_{H_i|H_{i-1}}$. The energy demand X_i is generated depending on the current hypothesis and the last energy demand (H_i, X_{i-1}) only and following the time-invariant conditional p.m.f. $p_{X_i|H_i,X_{i-1}}$. The EMU requests an energy supply Y_i from the EP depending on the current energy demand and ES state (X_i, Z_i) only and following an instantaneous energy management policy $\gamma_i : \mathcal{X} \times \mathcal{Z} \to \mathcal{Y}$ characterized by the conditional p.m.f. $p_{Y_i|X_i,Z_i}$. In this model, there are two constraints on an instantaneous energy management policy: The instantaneous energy demand x_i is always satisfied; and there is no energy wasted, i.e.,

$$z_i + y_i - x_i = z_{i+1},$$

which leads to

$$p_{Z_{i+1}|X_i,Z_i}(z_i + y_i - x_i | x_i, z_i) = p_{Y_i|X_i,Z_i}(y_i|x_i, z_i). \tag{6.1}$$

It means that Z_{i+1} depends on the current energy demand and ES state (X_i, Z_i) only and an energy management policy γ_i can be equivalently characterized by the conditional p.m.f. $p_{Z_{i+1}|X_i,Z_i}$. Because of these constraints, a feasible energy management policy γ_i has the following property:

$$\text{If } y_i < \max\{0, x_i - z_i\} \text{ or } y_i > m + x_i - z_i,\ p_{Y_i|X_i,Z_i}(y_i|x_i, z_i) = 0, \tag{6.2}$$

where the first condition indicates that the lower bound of the energy supply y_i is $x_i - z_i$ to provide the remaining energy when the ES state z_i cannot satisfy the energy demand x_i solely; and the second condition indicates that the upper bound of y_i is constrained by the ES capacity. Let Γ denote the set of feasible instantaneous energy management policies satisfying (6.2).

Since the consumer behavior hypothesis is allowed to be time-variant, an instantaneous privacy leakage at a time slot i is considered where the meter reading at the time slot Y_i is intercepted by an AD to infer the hypothesis H_i by making a guess $\hat{H}_i$, i.e., it is assumed that a decision $\hat{H}_i$ of the AD is made depending on Y_i only and following an instantaneous decision strategy characterized by the conditional p.m.f. $p_{\hat{H}_i|Y_i}$.

These dependence settings can be summarized as the following equation:

$$\begin{aligned} & p_{\hat{H}^k,H^k,X^k,Y^k,Z^k} \\ &= p_{H_1,X_1,Z_1} \prod_{i=1}^{k} p_{\hat{H}_i|Y_i} p_{Y_i|X_i,Z_i} \prod_{j=2}^{k} p_{Z_j|X_{j-1},Z_{j-1}} p_{X_j|H_j,X_{j-1}} p_{H_j|H_{j-1}}. \end{aligned} \tag{6.3}$$

6.2 Bayesian Hypothesis Testing Measure of Privacy Leakage

Following from the privacy-preserving objective of the smart meter system designer, the AD is assumed to be informed, e.g., the AD can be a compromised manager of the EP, and to have a full knowledge about the smart meter system statistics, e.g., the (conditional) p.m.f.s p_{H_1,X_1,Z_1}, $\left\{p_{H_i|H_{i-1}}\right\}_{i=2}^{\infty}$, $\left\{p_{X_i|H_i,X_{i-1}}\right\}_{i=2}^{\infty}$, and the energy management policies $\left\{p_{Y_i|X_i,Z_i}\right\}_{i=1}^{\infty}$. Based on the knowledge, the AD is further assumed to always use an optimal Bayesian hypothesis testing strategy at every time slot. Let $c(\hat{h}_i, h_i)$ denote the time-invariant decision cost of the AD to make a decision $\hat{h}_i$ when the correct behavior hypothesis is h_i. These decision costs are assigned also following the privacy-preserving design objective. As argued before, these assumptions on the AD will lead to optimal privacy-preserving energy management policies with a privacy-preserving performance guarantee. Given the statistical knowledge about the smart meter system, based on [61] and Remark 2.3, an optimal decision strategy of the AD at a time slot ϕ_i^* is the following deterministic likelihood-based test

$$\begin{aligned} \hat{H}_i &= \phi_i^*(y_i) \\ &= \arg\min_{\hat{h}_i \in \mathcal{H}} \sum_{h_i \in \mathcal{H}} p_{Y_i|H_i}(y_i|h_i) p_{H_i}(h_i) c(\hat{h}_i, h_i) \\ &= \arg\min_{\hat{h}_i \in \mathcal{H}} \sum_{(h_i,x_i,z_i) \in \mathcal{H}\times\mathcal{X}\times\mathcal{Z}} p_{Y_i|X_i,Z_i}(y_i|x_i,z_i) p_{H_i,X_i,Z_i}(h_i,x_i,z_i) c(\hat{h}_i, h_i). \end{aligned} \tag{6.4}$$

The corresponding minimal Bayesian risk $r_i(\phi_i^*)$ can be expressed in terms of p_{H_i,X_i,Z_i} and the energy management policy $p_{Y_i|X_i,Z_i}$ as

$$\begin{aligned} & r_i(\phi_i^*) \\ &= \sum_{y_i \in \mathcal{Y}} \min_{\hat{h}_i \in \mathcal{H}} \left\{ \sum_{(h_i,x_i,z_i) \in \mathcal{H}\times\mathcal{X}\times\mathcal{Z}} p_{Y_i|X_i,Z_i}(y_i|x_i,z_i) p_{H_i,X_i,Z_i}(h_i,x_i,z_i) c(\hat{h}_i, h_i) \right\}. \end{aligned} \tag{6.5}$$

The minimal Bayesian risk $r_i(\phi_i^*)$ measures the privacy leakage at time slot i. Intuitively, a privacy-preserving design of the instantaneous energy management policy is to maximize the minimal Bayesian risk $r_i(\phi_i^*)$. Due to the finite capacity of the ES and the utility constraint of always satisfying the energy demands without

any wasted energy, the energy management policy used at a time slot will affect the future statistics of the smart meter system, e.g., $p_{H_{i+1},X_{i+1},Z_{i+1}}$ partially depends on the energy management policy γ_i characterized by $p_{Z_{i+1}|X_i,Z_i}$. Therefore, successive independent optimization of energy management policy at every time slot does not necessarily lead to an optimal privacy-preserving design over the considered infinite time horizon. Instead, a privacy leakage measure over an infinite time horizon needs to be specified.

Over an infinite time horizon and given initial statistics p_{H_1,X_1,Z_1}, the privacy leakage of energy management policies $\{\gamma_i\}_{i=1}^{\infty} \in \Gamma^{\infty}$ is measured by the accumulated discounted minimal Bayesian risk as

$$V(p_{H_1,X_1,Z_1}, \{\gamma_i\}_{i=1}^{\infty}) \triangleq \sum_{i=1}^{\infty} \beta^{i-1} r_i(\phi_i^*), \tag{6.6}$$

where $0 < \beta < 1$ is a discount factor to ensure the convergence of the measure; the statistics $\{p_{H_i,X_i,Z_i}\}_{i=1}^{\infty}$ are determined by the initial statistics p_{H_1,X_1,Z_1} and the energy management policies $\{\gamma_i\}_{i=1}^{\infty}$; optimal strategies $\{\phi_i^*\}_{i=1}^{\infty}$ and minimal instantaneous Bayesian risks $\{r_i(\phi_i^*)\}_{i=1}^{\infty}$ of the AD are determined by the statistics $\{p_{H_i,X_i,Z_i}\}_{i=1}^{\infty}$ and the energy management policies $\{\gamma_i\}_{i=1}^{\infty}$ following (6.4) and (6.5). From the operational perspective, the proposed privacy leakage measure V is applicable in the scenarios where the privacy-preserving concern degrades as time goes on. For instance, the AD might need timely information about the consumer behaviors; or a longer time horizon means a higher exposure risk for the AD.

6.3 Privacy-Preserving Energy Management

Problem formulation

Using the proposed privacy leakage measure, the privacy-preserving objective is to design optimal energy management policies to maximize V: Given the initial statistics p_{H_1,X_1,Z_1},

$$\{\gamma_i^*\}_{i=1}^{\infty} = \underset{\{\gamma_i\}_{i=1}^{\infty} \in \Gamma^{\infty}}{\arg\max}\ V(p_{H_1,X_1,Z_1}, \{\gamma_i\}_{i=1}^{\infty}). \tag{6.7}$$

As discussed before, the current choice of the energy management policy will affect the future statistics of the smart meter system which in turn will affect the choices of the future energy management policies. In the following, a brief introduction of the MDP problem is given which can be adopted as a powerful tool to analyze the optimization problem (6.7).

Markov decision process

Conceptual foundations of the MDP problem and the extensions can be found in [27]. As illustrated in Figure 6.2, an MDP consists of the following elements:

1. A set of states: $s_i \in \mathcal{S}$,
2. A set of actions: $a_i \in \mathcal{A}$,
3. Time-invariant state transition: $p_{S_{i+1}|S_i,A_i}$,
4. Time-invariant rewards: $\{R_i(s_i, a_i)\}_{s_i \in \mathcal{S}, a_i \in \mathcal{A}}$.

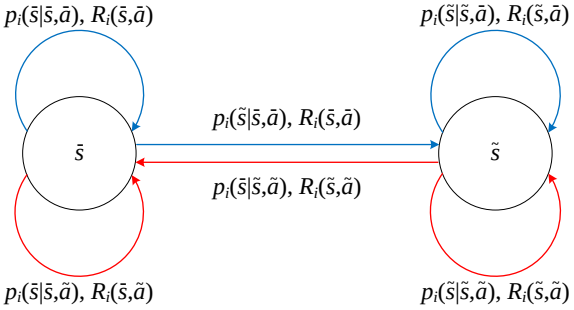


Figure 6.2: Illustration of an MDP where the state alphabet is $\mathcal{S} = \{\bar{s}, \tilde{s}\}$; there are two possible actions $\bar{a}$ and $\tilde{a}$; the state transitions by using action $\bar{a}$ are represented by blue arrows; the state transitions by using action $\tilde{a}$ are represented by red arrows. Note that a simplified notation p_i is used to denote $p_{S_{i+1}|S_i,A_i}$ in the illustration.

At a time slot i, denote a (randomized) policy by δ_i which maps a state observation s_i to an action a_i following the corresponding conditional p.m.f. $p_{A_i|S_i}$. Let Δ denote the set of feasible policies. An MDP problem over an infinite time horizon is to find optimal policies $\{\delta_i^*\}_{i=1}^{\infty}$ which maximize an expected accumulated discounted reward:

$$\{\delta_i^*\}_{i=1}^{\infty} = \underset{\{\delta_i\}_{i=1}^{\infty} \in \Delta^{\infty}}{\arg\max}\ J(s_1, \{\delta_i\}_{i=1}^{\infty}), \tag{6.8}$$

where $s_1 \in \mathcal{S}$ denotes the initial state; the expected accumulated discounted reward is

$$J(s_1, \{\delta_i\}_{i=1}^{\infty}) = \mathrm{E}\left[\sum_{i=1}^{\infty} \alpha^{i-1} R_i(S_i, \delta_i(S_i))\right]; \tag{6.9}$$

and the discount factor α satisfies $0 < \alpha < 1$. Given an initial state $s_1 \in \mathcal{S}$, denote the maximum expected accumulated discounted reward by $J^*(s_1)$, i.e., $J^*(s_1) = J(s_1, \{\delta_i^*\}_{i=1}^{\infty})$.

At time slot k and given a state observation $s_k \in \mathcal{S}$, a Bellman equation can be formulated as

$$J^*(s_k) = \max_{a_k \in \mathcal{A}} R_k(s_k, a_k) + \alpha \cdot \sum_{s_{k+1} \in \mathcal{S}} J^*(s_{k+1}) \cdot p_{S_{k+1}|S_k,A_k}(s_{k+1}|s_k, a_k). \tag{6.10}$$

Then, an optimal policy δ_k^* at time slot k is a deterministic map: Given $s_k \in \mathcal{S}$,

$$\delta_k^*(s_k) = \arg\max_{a_k \in \mathcal{A}} R_k(s_k, a_k) + \alpha \cdot \sum_{s_{k+1} \in \mathcal{S}} J^*(s_{k+1}) \cdot p_{S_{k+1}|S_k, A_k}(s_{k+1}|s_k, a_k). \quad (6.11)$$

Since the reward function and the random state transition are time-invariant, the optimal policy is also time-invariant. The solutions of $\{J^*(s_1)\}_{s_1 \in \mathcal{S}}$ and $\{\delta_i^*\}_{i=1}^{\infty}$ can be obtained through a value iteration algorithm or a policy iteration algorithm [27]. The value iteration algorithm is presented in Algorithm 6.1.

Algorithm 6.1 Value iteration algorithm.

1: input a reward vector $[J^*(s_{(1)}), \ldots, J^*(s_{(||\mathcal{S}||)})]$.
2: **while** the update of reward vector does not satisfy convergence criterion **do**
3: **for** $t \in \{1, \ldots, ||\mathcal{S}||\}$ **do**
4:

$$J(s_{(t)}) \leftarrow \max_{a_i \in \mathcal{A}} R_i(s_{(t)}, a_i) + \alpha \sum_{s_{i+1} \in \mathcal{S}} J^*(s_{i+1}) \cdot p_{S_{i+1}|S_i, A_i}(s_{i+1}|s_{(t)}, a_i)$$

$$\delta_i^*(s_{(t)}) \leftarrow \arg\max_{a_i \in \mathcal{A}} R_i(s_{(t)}, a_i) + \alpha \sum_{s_{i+1} \in \mathcal{S}} J^*(s_{i+1}) \cdot p_{S_{i+1}|S_i, A_i}(s_{i+1}|s_{(t)}, a_i)$$

$$J^*(s_{(t)}) \leftarrow J(s_{(t)}).$$

5: **end for**
6: **end while**
output: the updated reward vector $[J^*(s_{(1)}), \ldots, J^*(s_{(||\mathcal{S}||)})]$ and the policy vector $[\delta_i^*(s_{(1)}), \ldots, \delta_i^*(s_{(||\mathcal{S}||)})]$

Identification of Markov decision process elements

In the following, it is shown that the energy management of the smart meter system can be identified as an MDP.

From the settings in Section 6.1, it follows that

$$p_{H_{i+1}, X_{i+1}, Z_{i+1}|H_i, X_i, Z_i} = p_{Z_{i+1}|X_i, Z_i} p_{X_{i+1}|H_{i+1}, X_i} p_{H_{i+1}|H_i}. \quad (6.12)$$

Since the p.m.f. $p_{Z_{i+1}|X_i, Z_i}$ represents an energy management policy γ_i, the transition from (H_i, X_i, Z_i) to $(H_{i+1}, X_{i+1}, Z_{i+1})$ depends on the used energy management policy. On observing p_{H_i, X_i, Z_i}, if an energy management policy characterized by $p_{Z_{i+1}|X_i, Z_i}$ is used, the EMU can determine (observe) $p_{H_{i+1}, X_{i+1}, Z_{i+1}}$ as

$$p_{H_{i+1}, X_{i+1}, Z_{i+1}} = (p_{Z_{i+1}|X_i, Z_i} p_{X_{i+1}|H_{i+1}, X_i} p_{H_{i+1}|H_i}) \circ p_{H_i, X_i, Z_i}, \quad (6.13)$$

where "$\circ$" denotes the composition operation.

From (6.5), the minimal Bayesian risk $r_i(\phi_i^*)$ is in terms of the energy management policy characterized by $p_{Y_i|X_i,Z_i}$ and the statistics p_{H_i,X_i,Z_i}.

These observations indicate an MDP formulation of the energy management of the smart meter system. In the following discussion, there is a little abuse of notation.

Proposition 6.1. *The energy management of the smart meter system can be seen as a belief state MDP.*

Explicit identification of elements of the belief state MDP is still required and is shown in the following constructive proof of Proposition 6.1.

Proof. Elements of the belief state MDP are identified as:

1. A set of states: $s_i = (h_i, x_i, z_i)$ and $s_i \in \mathcal{S} = \mathcal{H} \times \mathcal{X} \times \mathcal{Z}$,

2. A set of belief states: $b_i = p_{H_i,X_i,Z_i}$ and $b_i \in \mathcal{B}$,

3. A set of actions: $a_i = p_{Y_i|X_i,Z_i}$ and $a_i \in \Gamma$,

4. Time-invariant belief state transition:

$$p_{B_{i+1}|B_i,A_i}(b_{i+1}|b_i,a_i) = \begin{cases} 1, \text{ if } b_{i+1} = p_{S_{i+1}|S_i} \circ b_i \\ 0, \text{ otherwise} \end{cases},$$

   where $p_{S_{i+1}|S_i} = p_{Z_{i+1}|X_i,Z_i} p_{X_{i+1}|H_{i+1},X_i} p_{H_{i+1}|H_i}$ and $p_{Z_{i+1}|X_i,Z_i}$ can be substituted by a_i according to (6.1),

5. Time-invariant rewards: $\{R_i(b_i,a_i)\}_{b_i \in \mathcal{B}, a_i \in \Gamma}$ where $R_i(b_i,a_i) = r_i(\phi_i^*)$.

□

A belief state here denotes a probability distribution of the state. An action in the belief state MDP is an energy management policy. A reward is the minimal Bayesian risk of the AD. Different from the introduced basic MDP, the reward in the belief state MDP depends on the belief state instead of the observation of state; the belief state transition is deterministic given a current belief state and a current action.

The belief state MDP formulation of the energy management in the smart meter system implies that standard methods can be used to obtain or to approximate optimal privacy-preserving energy management policies for the problem (6.7).

Optimal privacy-preserving energy management

For the belief state MDP problem, denote a (randomized) policy δ_i which maps a belief state b_i to an action a_i (or equivalently an energy management policy γ_i) following $p_{A_i|B_i}$. Let Δ be the set of feasible policies. Given an initial belief state $b_1 \in \mathcal{B}$, consider the following belief state MDP problem:

$$\{\delta_i^*\}_{i=1}^{\infty} = \underset{\{\delta_i\}_{i=1}^{\infty} \in \Delta^{\infty}}{\arg\max} \; J(b_1, \{\delta_i\}_{i=1}^{\infty}), \tag{6.14}$$

where the expected accumulated discounted reward is

$$J(b_1, \{\delta_i\}_{i=1}^{\infty}) = \mathrm{E}\left[\sum_{i=1}^{\infty} \beta^{i-1} R_i(B_i, \delta_i(B_i))\right]. \tag{6.15}$$

Theorem 6.1. *The belief state MDP problem (6.14) is equivalent to the optimization problem (6.7).*

Proof. For the belief state MDP problem (6.14), it is sufficient to consider deterministic time-invariant optimal policies $\{\delta_i^*\}_{i=1}^{\infty}$ at all time slots. Let Δ^{D} denote the set of deterministic policies. Then the belief state MDP problem (6.14) can be equivalently rewritten as

$$\{\delta_i^*\}_{i=1}^{\infty} = \underset{\{\delta_i\}_{i=1}^{\infty} \in \Delta^{\mathrm{D}\infty}}{\arg\max} \; J(b_1, \{\delta_i\}_{i=1}^{\infty}),$$

where the expected accumulated discounted reward reduces to

$$J(b_1, \{\delta_i\}_{i=1}^{\infty}) = \sum_{i=1}^{\infty} \beta^{i-1} R_i(b_i, \delta_i(b_i)).$$

It means that the optimization of an energy management policy γ_i depends on the statistical information p_{H_i,X_i,Z_i} only. Compared with the belief state MDP problem, the privacy-preserving optimization of γ_i in (6.7) depends on all available statistical information p_{H_1,X_1,Z_1} and $\{\gamma_j\}_{j=1}^{i-1}$. Note that p_{H_1,X_1,Z_1}, $\{\gamma_j\}_{j=1}^{i-1}$ jointly determine $\{p_{H_j,X_j,Z_j}\}_{j=1}^{i}$; and the optimization of the remaining energy management policies $\{\gamma_j\}_{j=i}^{\infty}$ depends on p_{H_i,X_i,Z_i} only. It means that the privacy-preserving optimization of γ_i in (6.7) depends on the sufficient statistic p_{H_i,X_i,Z_i}. Therefore, the belief state MDP problem and the privacy-preserving optimization problem are equivalent: $\gamma_i^* = a_i^* = \delta_i^*(b_i^*)$ and $J(b_1, \{\delta_i^*\}_{i=1}^{\infty}) = V(b_1, \{\gamma_i^*\}_{i=1}^{\infty})$. □

Given $b_1 \in \mathcal{B}$, let $J^*(b_1) = J(b_1, \{\delta_i^*\}_{i=1}^{\infty})$. From Bellman's principle of optimality [5], it follows that for all $k \geq 1$ and $b_k \in \mathcal{B}$

$$\begin{aligned} J^*(b_k) &= \max_{a_k \in \Gamma} R_k(b_k, a_k) + \beta \cdot \sum_{b_{k+1} \in \mathcal{B}} J^*(b_{k+1}) p_{B_{k+1}|B_k,A_k}(b_{k+1}|b_k, a_k) \\ &= \max_{a_k \in \Gamma} R_k(b_k, a_k) + \beta \cdot J^*((\underbrace{p_{Z_{k+1}|X_k,Z_k}}_{a_k} p_{X_{k+1}|H_{k+1},X_k} p_{H_{k+1}|H_k}) \circ b_k), \end{aligned} \tag{6.16}$$

and

$$\delta_k^*(b_k) = \arg\max_{a_k \in \Gamma} R_k(b_k, a_k) + \beta \cdot J^*((\underbrace{p_{Z_{k+1}|X_k,Z_k}}_{a_k} p_{X_{k+1}|H_{k+1},X_k} p_{H_{k+1}|H_k}) \circ b_k). \tag{6.17}$$

From the same arguments, the optimal policies $\{\delta_i^*\}_{i=1}^{\infty}$ of the belief state MDP problem (6.14) are time-invariant and deterministic maps. Generally, solving the Bellman equation (6.16) is computationally complex due to the infinite alphabets of belief state and action. An approximation idea is to use some discretization procedure, e.g., using α-vector algorithm [51] by discretizing the action domain, using value iteration algorithm by discretizing both the belief state and action alphabets.

Remark 6.1. *With the time-invariant deterministic optimal policies $\{\delta_i^*\}_{i=1}^{\infty}$, the optimal privacy-preserving energy management policies $\{\gamma_i^*\}_{i=1}^{\infty}$ of (6.7) can be determined as follows: At the first time slot, the optimal energy management policy is*

$$\gamma_1^* = \delta_1^*(p_{H_1,X_1,Z_1});$$

determine belief state in the beginning of the second slot as

$$p_{H_2,X_2,Z_2}^* = (\underbrace{p_{Z_2|X_1,Z_1}^*}_{\gamma_1^*} p_{X_2|H_2,X_1} p_{H_2|H_1}) \circ p_{H_1,X_1,Z_1};$$

repeat the same steps at the following slots.

Instantaneous optimal energy management

Due to the computational complexity of the formulated belief state MDP problem, an instantaneous optimal energy management is also considered. At every time slot, an energy management policy is used to suppress the instantaneous privacy leakage through maximizing the minimal Bayesian risk of the AD without a concern about the impact on the further privacy leakage. At time slot i, denote an instantaneous optimal policy by $\delta_i^{\#}$ which maps a belief state b_i (or equivalently p_{H_i,X_i,Z_i}) to an action a_i (or equivalently an energy management policy γ_i) as

$$\delta_i^{\#}(b_i) = \arg\max_{a_i \in \Gamma} R_i(b_i, a_i). \tag{6.18}$$

The problem (6.18) is not a convex optimization. However, it can be rewritten as a set of linear programming problems as discussed in the following.

From (6.4), an optimal decision strategy ϕ_i^* for the AD at time slot i is a deterministic likelihood-based test. Thus, it is sufficient to consider a deterministic strategy for the AD. There are $l = ||\mathcal{H}||^{||\mathcal{Y}||} = n^{u+m+1}$ deterministic hypothesis testing strategies mapping from $\mathcal{Y}$ to $\mathcal{H}$. Let $\phi_{(j)} : \mathcal{Y} \to \mathcal{H}$ with $j \in \{1, \ldots, l\}$

denote the j-th deterministic decision strategy of the AD. Given a belief state b_i and a deterministic decision strategy $\phi_{(j)}$, define a subset of Γ as

$$\begin{aligned}&\Gamma_{(j)}(b_i)\\ &\triangleq \left\{ a_i \left| \forall (y_i, \hat{h}_i) \in \mathcal{Y} \times \mathcal{H}, \sum_{s_i \in \mathcal{S}} \left\{ (c(\phi_{(j)}(y_i), h_i) - c(\hat{h}_i, h_i)) a_i(y_i|x_i, z_i) b_i(s_i) \right\} \leq 0 \right. \right\}.\end{aligned}$$

From the definition, the subset $\Gamma_{(j)}(b_i)$ consists of actions (or equivalently energy management policies), any of which jointly with the given belief state b_i leads to that the deterministic strategy $\phi_{(j)}$ is an optimal strategy ϕ_i^* of the AD. It is obvious that a subset $\Gamma_{(j)}(b_i)$ is defined by linear constraints on a_i. In addition, it can be verified that $\bigcup_{j=1}^{l} \Gamma_{(j)}(b_i) = \Gamma$.

The non-convex optimization problem in (6.18) can be rewritten as

$$\delta_i^{\#}(b_i) = \max_{j \in \{1,\ldots,l\}} \left\{ \arg\max_{a_i \in \Gamma_{(j)}(b_i)} R_i(b_i, a_i) \right\}. \tag{6.19}$$

Proposition 6.2. *All inner optimizations of (6.19) are linear programmings.*

Proof. For the j-th inner optimization in (6.19), the objective $R_i(b_i, a_i)$ is maximized over a subset $\Gamma_{(j)}(b_i)$. From the definition of $\Gamma_{(j)}(b_i)$, the objective in the j-th inner optimization can be specified as

$$R_i(b_i, a_i) = \sum_{y_i \in \mathcal{Y}} \sum_{s_i \in \mathcal{S}} \left\{ c(\phi_{(j)}(y_i), h_i) a_i(y_i|x_i, z_i) b_i(s_i) \right\}.$$

It is obvious the specified objective is a linear function of a_i. In addition, the subset $\Gamma_{(j)}(b_i)$ is defined by a set of linear constraints on a_i. Therefore, any inner optimization in (6.19) is a linear programming to maximize a linear objective of a_i subject to a set of linear constraints on a_i. □

Using standard methods, the inner linear programmings can be efficiently solved. The outer optimization of (6.19) simply compares the results of the inner optimizations to determine the maximum instantaneous minimal Bayesian risk of the AD and the action $\delta_i^{\#}(b_i)$.

Remark 6.2. *The instantaneous optimal policies $\{\delta_i^{\#}\}_{i=1}^{\infty}$ are time-invariant.*

Remark 6.3. *With the time-invariant instantaneous optimal policies $\{\delta_i^{\#}\}_{i=1}^{\infty}$, the instantaneous optimal privacy-preserving energy management policies $\{\gamma_i^{\#}\}_{i=1}^{\infty}$ can be determined successively as follows: At the first time slot, the instantaneous optimal energy management policy is*

$$\gamma_1^{\#} = \delta_1^{\#}(p_{H_1, X_1, Z_1});$$

Table 6.1: Parameter settings of the numerical example.

parameter	value
n	2
u	1
m	1
β	0.5
$c(0,0) = c(1,1)$	0
$c(0,1) = c(1,0)$	1
$p_{H_i\|H_{i-1}}(0\|0)$	0.9
$p_{H_i\|H_{i-1}}(0\|1)$	0.2
$p_{X_i\|H_i,X_{i-1}}(0\|0,0)$	0.7
$p_{X_i\|H_i,X_{i-1}}(0\|0,1)$	0.3
$p_{X_i\|H_i,X_{i-1}}(0\|1,0)$	0.7
$p_{X_i\|H_i,X_{i-1}}(0\|1,1)$	0.3

determine belief state in the beginning of the second slot as

$$p^{\#}_{H_2,X_2,Z_2} = (\underbrace{p^{\#}_{Z_2|X_1,Z_1}}_{\gamma_1^{\#}} p_{X_2|H_2,X_1} p_{H_2|H_1}) \circ p_{H_1,X_1,Z_1};$$

repeat the same steps at the following slots.

6.4 Numerical Example

Here, a simple numerical example shows the privacy-preserving improvement of optimal energy management policies compared with instantaneous optimal energy management policies. The parameter settings of the smart meter system are listed in Table 6.1.

Since the belief state alphabet $\mathcal{B}$ is infinite, an approximation used here is to consider a finite number of discrete belief states as listed in Table 6.2. Here, the initial belief state p_{H_1,X_1,Z_1} can be the 12-th belief state $b_{(12)}$ or the 19-th belief state $b_{(19)}$. With the finite number of discrete belief states, the value iteration algorithm can be reduced to a set of linear programmings.

In Figure 6.3, the i-th square/circle is $J_i^{\#}(b_1) = \sum_{k=1}^{i} \beta^{k-1} R_k(b_k^{\#}, \delta_k^{\#}(b_k^{\#}))$ which denotes the accumulated discounted minimal Bayesian risk of the AD until time slot i by using instantaneous optimal policies. A solid line represents $J^*(b_1)$ by using optimal privacy-preserving energy management policies over the infinite time horizon. For this example, the numerical results indicate that the instantaneous optimal energy management policies can approach the privacy-preserving performance of the optimal energy management policies asymptotically.

Table 6.2: Discrete belief states.

index	non-zero probability	value
$b_{(1)}$	$p_{H_i,X_i,Z_i}(1,1,1)$	1
$b_{(2)}$	$p_{H_i,X_i,Z_i}(1,1,0) = p_{H_i,X_i,Z_i}(1,1,1)$	0.5
$b_{(3)}$	$p_{H_i,X_i,Z_i}(1,1,0)$	1
$b_{(4)}$	$p_{H_i,X_i,Z_i}(1,0,1) = p_{H_i,X_i,Z_i}(1,1,1)$	0.5
$b_{(5)}$	$p_{H_i,X_i,Z_i}(1,0,1) = p_{H_i,X_i,Z_i}(1,1,0)$	0.5
$b_{(6)}$	$p_{H_i,X_i,Z_i}(1,0,1)$	1
$b_{(7)}$	$p_{H_i,X_i,Z_i}(1,0,0) = p_{H_i,X_i,Z_i}(1,1,1)$	0.5
$b_{(8)}$	$p_{H_i,X_i,Z_i}(1,0,0) = p_{H_i,X_i,Z_i}(1,1,0)$	0.5
$b_{(9)}$	$p_{H_i,X_i,Z_i}(1,0,0) = p_{H_i,X_i,Z_i}(1,0,1)$	0.5
$b_{(10)}$	$p_{H_i,X_i,Z_i}(1,0,0)$	1
$b_{(11)}$	$p_{H_i,X_i,Z_i}(0,1,1) = p_{H_i,X_i,Z_i}(1,1,1)$	0.5
$b_{(12)}$	$p_{H_i,X_i,Z_i}(0,1,1) = p_{H_i,X_i,Z_i}(1,1,0)$	0.5
$b_{(13)}$	$p_{H_i,X_i,Z_i}(0,1,1) = p_{H_i,X_i,Z_i}(1,0,1)$	0.5
$b_{(14)}$	$p_{H_i,X_i,Z_i}(0,1,1) = p_{H_i,X_i,Z_i}(1,0,0)$	0.5
$b_{(15)}$	$p_{H_i,X_i,Z_i}(0,1,1)$	1
$b_{(16)}$	$p_{H_i,X_i,Z_i}(0,1,0) = p_{H_i,X_i,Z_i}(1,1,1)$	0.5
$b_{(17)}$	$p_{H_i,X_i,Z_i}(0,1,0) = p_{H_i,X_i,Z_i}(1,1,0)$	0.5
$b_{(18)}$	$p_{H_i,X_i,Z_i}(0,1,0) = p_{H_i,X_i,Z_i}(1,0,1)$	0.5
$b_{(19)}$	$p_{H_i,X_i,Z_i}(0,1,0) = p_{H_i,X_i,Z_i}(1,0,0)$	0.5
$b_{(20)}$	$p_{H_i,X_i,Z_i}(0,1,0) = p_{H_i,X_i,Z_i}(0,1,1)$	0.5
$b_{(21)}$	$p_{H_i,X_i,Z_i}(0,1,0)$	1
$b_{(22)}$	$p_{H_i,X_i,Z_i}(0,0,1) = p_{H_i,X_i,Z_i}(1,1,1)$	0.5
$b_{(23)}$	$p_{H_i,X_i,Z_i}(0,0,1) = p_{H_i,X_i,Z_i}(1,1,0)$	0.5
$b_{(24)}$	$p_{H_i,X_i,Z_i}(0,0,1) = p_{H_i,X_i,Z_i}(1,0,1)$	0.5
$b_{(25)}$	$p_{H_i,X_i,Z_i}(0,0,1) = p_{H_i,X_i,Z_i}(1,0,0)$	0.5
$b_{(26)}$	$p_{H_i,X_i,Z_i}(0,0,1) = p_{H_i,X_i,Z_i}(0,1,1)$	0.5
$b_{(27)}$	$p_{H_i,X_i,Z_i}(0,0,1) = p_{H_i,X_i,Z_i}(0,1,0)$	0.5
$b_{(28)}$	$p_{H_i,X_i,Z_i}(0,0,1)$	1
$b_{(29)}$	$p_{H_i,X_i,Z_i}(0,0,0) = p_{H_i,X_i,Z_i}(1,1,1)$	0.5
$b_{(30)}$	$p_{H_i,X_i,Z_i}(0,0,0) = p_{H_i,X_i,Z_i}(1,1,0)$	0.5
$b_{(31)}$	$p_{H_i,X_i,Z_i}(0,0,0) = p_{H_i,X_i,Z_i}(1,0,1)$	0.5
$b_{(32)}$	$p_{H_i,X_i,Z_i}(0,0,0) = p_{H_i,X_i,Z_i}(1,0,0)$	0.5
$b_{(33)}$	$p_{H_i,X_i,Z_i}(0,0,0) = p_{H_i,X_i,Z_i}(0,1,1)$	0.5
$b_{(34)}$	$p_{H_i,X_i,Z_i}(0,0,0) = p_{H_i,X_i,Z_i}(0,1,0)$	0.5
$b_{(35)}$	$p_{H_i,X_i,Z_i}(0,0,0) = p_{H_i,X_i,Z_i}(0,0,1)$	0.5
$b_{(36)}$	$p_{H_i,X_i,Z_i}(0,0,0)$	1

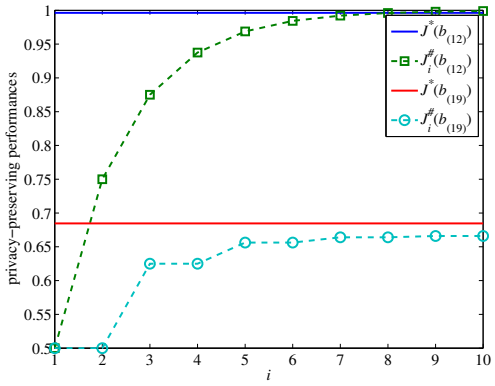


Figure 6.3: Privacy-preserving performance comparison between using optimal energy management policies and using instantaneous optimal energy management policies.

6.5 Summary

In this chapter, the privacy-preserving energy management of a finite-capacity ES is studied. At a time slot, the instantaneous privacy leakage risk is measured by the minimal Bayesian risk of the AD. Over an infinite time horizon, optimal privacy-preserving energy management policies are designed to maximize the privacy leakage measure of an accumulated discounted minimal Bayesian risk of the AD. The energy management in the smart meter system is identified as a belief state MDP. Then, a belief state MDP problem is formulated for the optimization of privacy-preserving energy management policies and established standard algorithms can be used to design the optimal privacy-preserving energy management policies. Without considering the impact on the future, an instantaneous optimal privacy-preserving energy management policy suppresses the instantaneous privacy leakage or equivalently maximizes the minimal Bayesian risk of the AD at the slot. It is shown that an instantaneous optimal privacy-preserving energy management policy can be obtained by solving a set of linear programmings.

Chapter 7

Conclusion

In this thesis, privacy-by-design approaches for cyber-physical system are investigated in the contexts of sensor networks and smart meter systems. Privacy-by-design approaches are realized by privacy-preserving designs of the physical-layer operations. Hypothesis testing measures are used to assess physical-layer operations and privacy leakages. This work focuses on the optimality characteristics of privacy-preserving designs, (asymptotic) optimal privacy-preserving performances, and privacy-preserving design algorithms.

The physical-layer operation of a sensor network is modeled as a distributed hypothesis test. An informed eavesdropper is assumed to intercept the open-access remote decisions and the privacy leakage is measured by the hypothesis testing performance of the eavesdropper. The privacy-by-design approach is realized through an optimal privacy-preserving design of the distributed hypothesis testing network with the objectives to improve the hypothesis testing performance of the fusion center and to suppress the hypothesis testing performance of the eavesdropper. In an optimal privacy-preserving distributed Bayesian hypothesis testing design, it is shown that the optimality of deterministic likelihood-based test (or likelihood-ratio test) holds for the protected remote decision makers and for the fusion center; while a randomized decision strategy of two deterministic likelihood-based tests might outperform deterministic likelihood-based tests for an intercepted remote decision make. It is further shown that a randomized remote decision strategy in an optimal privacy-preserving distributed Bayesian hypothesis testing network is completely characterized by the privacy-preserving condition. These optimality characteristics are used to simplify the proposed extend person-by-person optimization algorithms. In an optimal privacy-constrained Neyman-Pearson design of a particular distributed binary hypothesis testing network, the optimality of deterministic likelihood-ratio test holds for both remote decision makers if the false-alarm probability upper bounds of fusion decision and eavesdropper decision are the same. The work on privacy-preserving distributed hypothesis tests can be extended in many aspects, e.g., in a sequential hypothesis testing scenario or under an uncertainty

about the intercepted remote decision makers.

Smart meter privacy leakage can be suppressed through adding distortions on the meter readings to hide the real energy demand profile. Here, the privacy-by-design approach is realized through an optimal privacy-preserving energy management of renewable energy supplies or charging/discharging energy flows of a finite-capacity energy storage. In the presence of an ideal renewable energy source, it is shown that an optimal asymptotic privacy-preserving performance can be characterized by a Kullback-Leibler divergence rate under an adversarial Neyman-Pearson hypothesis testing privacy leakage, or by a Chernoff information rate under an adversarial Bayesian hypothesis testing privacy leakage. Particularly, an optimal memoryless hypothesis-aware energy management uses time-invariant policies at all time slots and the corresponding asymptotic privacy-preserving performance is characterized by a single-letter Kullback-Leibler divergence or by a single-letter Chernoff information. Under both adversarial hypothesis testing privacy leakage scenarios, asymptotic privacy-preserving performance comparisons of memoryless hypothesis-aware policy and hypothesis-unaware policy with memory show that the correct hypothesis information cannot be more useful than all available energy demand and supply data. In the presence of a finite-capacity energy storage, it is shown that the privacy-preserving energy management can be cast to a belief state Markov decision process to deal with the memory in the smart meter system. Then, a belief state Markov decision process problem is formulated for the optimization of privacy-preserving energy management policies and the value iteration algorithm can be used to design optimal energy management policies. The work on the privacy-preserving energy management can also be extended in many aspects. The hypothesis in the smart meter privacy problems can be generalized to be more than binary. Instead of considering privacy leakage suppression only, utility objectives, e.g., cost saving of the consumer or prediction accuracy of the energy provider, should also be taken into account in the energy management design.

This work contributes to realization of the privacy-by-design approach in the following aspects: Novel problems are formulated for privacy-preserving physical-layer design; optimal privacy-preserving designs and performances are characterized; design algorithms are proposed. The idea of privacy-preserving physical-layer design, the used methods, and the obtained results in this work can be applied or extended for the other cyber-physical systems other than the considered sensor networks and smart meter systems. The smartness of cyber-physical systems will bring great benefits to our livings and environments while the privacy issue is a key to determine the success of cyber-physical systems. This work provides a new point of view to tradeoff smartness and privacy.

Bibliography

[1] URL `http://www.eugdpr.org/`.

[2] Every convex function is locally Lipschitz. *The American Mathematical Monthly*, 79(10):1121–1124, 1972.

[3] T. C. Aysal and K. E. Barner. Sensor data cryptography in wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, 3(2): 273–289, 2008.

[4] R. F. Barber and J. C. Duchi. Privacy and statistical risk: Formalisms and minimax bounds. eprint arXiv:1412.4451.

[5] R. Bellman. The theory of dynamic programming. *Bulletin of the American Mathematical Society*, 60(6):503–516, 1954.

[6] D. Bertsimas and J. N. Tsitsiklis. *Introduction to Linear Optimization*. Athena Scientific, 1997.

[7] R. S. Blum, S. A. Kassam, and H. V. Poor. Distributed detection with multiple sensors: Part II - Advanced topics. *Proceedings of the IEEE*, 85(1):64–79, 1997.

[8] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.

[9] Z. Cao, J. Hu, Z. Chen, M. Xu, and X. Zhou. Feedback: Towards dynamic behavior and secure routing for wireless sensor networks. In *Proceedings of AINA 2006*, pages 160–164, 2006.

[10] P.-N. Chen. General formulas for the Neyman-Pearson Type-II error exponent subject to fixed and exponential Type-I error bounds. *IEEE Transactions on Information Theory*, 42(1):316–323, 1996.

[11] H. Chernoff. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *The Annals of Mathematical Statistics*, 23(4): 493–507, 1952.

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

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

[14] C. Dwork. Differential privacy. In *Proceedings of ICALP 2006*, pages 1–12, 2006.

[15] 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*, pages 7216–7221, 2015.

[16] S. Goel and R. Negi. Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications*, 7(6):2180–2189, 2008.

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

[18] X. Guo, A. S. Leong, and S. Dey. Estimation in wireless sensor networks with security constraints. *IEEE Transactions on Aerospace and Electronic Systems*, PP(99):1–1, 2017.

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

[20] I. Y. Hoballah and P. K. Varshney. Distributed Bayesian signal detection. *IEEE Transactions on Information Theory*, 35(5):995–1000, 1989.

[21] H. Jeon, J. Choi, S. W. McLaughlin, and J. Ha. Channel aware encryption and decision fusion for wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, 8(4):619–625, 2013.

[22] H. Jeon, D. Hwang, J. Choi, H. Lee, and J. Ha. Secure type-based multiple access. *IEEE Transactions on Information Forensics and Security*, 6(3):763–774, 2011.

[23] Z. Ji, Z. C. Lipton, and C. Elkan. Differential privacy and machine learning: A survey and review. eprint arXiv:1412.7584.

[24] P. Kairouz, S. Oh, and P. Viswanath. The composition theorem for differential privacy. In *Proceedings of the 32nd International Conference on Machine Learning*, pages 1–10, 2015.

[25] 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*, pages 232–237, 2010.

[26] K. Kittichokechai, T. J. Oechtering, and M. Skoglund. Secure source coding with action-dependent side information. In *Proceedings of ISIT 2011*, pages 1678–1682, 2011.

[27] V. Krishnamurthy. *Partially Observed Markov Decision Processes: From Filtering to Controlled Sensing*. Cambridge University Press, 2016.

[28] J. Le Ny and G. J. Pappas. Differentially private filtering. *IEEE Transactions on Automatic Control*, 59(2):341–354, 2014.

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

[30] S. Li, A. Khisti, and A. Mahajan. Structure of optimal privacy-preserving policies in smart-metered systems with a rechargeable battery. In *Proceedings of SPAWC 2015*, pages 375–379, 2015.

[31] Z. Li and T. J. Oechtering. Differential privacy in parallel distributed Bayesian detections. In *Proceedings of Fusion 2014*, pages 1–7, 2014.

[32] Z. Li and T. J. Oechtering. Privacy-concerned parallel distributed Bayesian sequential detection. In *Proceedings of GlobalSIP 2014*, pages 928–932, 2014.

[33] Z. Li and T. J. Oechtering. Tandem distributed Bayesian detection with privacy constraints. In *Proceedings of ICASSP 2014*, pages 8168–8172, 2014.

[34] Z. Li and T. J. Oechtering. Privacy-aware distributed Bayesian detection. *IEEE Journal of Selected Topics in Signal Processing*, 9(7):1345–1357, 2015.

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

[36] Z. Li and T. J. Oechtering. Privacy-constrained parallel distributed Neyman-Pearson test. *IEEE Transactions on Signal and Information Processing over Networks*, 3(1):77–90, 2017.

[37] Z. Li, T. J. Oechtering, and D. Gündüz. Smart meter privacy: Adversarial hypothesis testing models. In Preparation for IEEE Transactions on Information Forensics and Security.

[38] Z. Li, T. J. Oechtering, and D. Gündüz. Smart meter privacy based on adversarial hypothesis testing. Accepted at ISIT 2017.

[39] Z. Li, T. J. Oechtering, and J. Jaldén. Parallel distributed Neyman-Pearson detection with privacy constraints. In *Proceedings of ICC 2014 Workshop*, pages 765–770, 2014.

[40] Z. Li, T. J. Oechtering, and K. Kittichokechai. Parallel distributed Bayesian detection with privacy constraints. In *Proceedings of ICC 2014*, pages 2178–2183, 2014.

[41] Z. Li, T. J. Oechtering, and M. Skoglund. Privacy-preserving energy flow control in smart grids. In *Proceedings of ICASSP 2016*, pages 2194–2198, 2016.

[42] D. Liu, P. Ning, S. Zhu, and S. Jajodia. Practical broadcast authentication in sensor networks. In *Proceedings of MobiQuitous 2005*, pages 118–129, 2005.

[43] S. Marano, V. Matta, and P. K. Willett. Distributed detection with censoring sensors under physical layer secrecy. *IEEE Transactions on Signal Processing*, 57(5):1976–1986, 2009.

[44] M. Mhanna and P. Piantanida. On secure distributed hypothesis testing. In *Proceedings of ISIT 2015*, pages 1605–1609, 2015.

[45] 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*, pages 61–66, 2010.

[46] V. Nadendla. Secure distributed detection in wireless sensor networks via encryption of sensor decision. Master's thesis, Louisiana State University, 2009.

[47] V. S. S. Nadendla, H. Chen, and P. K. Varshney. Secure distributed detection in the presence of eavesdroppers. In *Proceedings of ASILOMAR 2010*, pages 1437–1441, 2010.

[48] F. Nielsen. An information-geometric characterization of Chernoff information. *IEEE Signal Processing Letters*, 20(3):269–272, 2013.

[49] H. Nikaidô. On von Neumann's minimax theorem. *Pacific Journal of Mathematics*, 4(1):65–72, 1954.

[50] S. Schmidt, H. Krahn, S. Fischer, and D. Wätjen. A security architecture for mobile wireless sensor networks. In *Proceedings of the First European Conference on Security in Ad-hoc and Sensor Networks*, pages 166–177, 2005.

[51] R. D. Smallwood and E. J. Sondik. The optimal control of partially observable Markov processes over a finite horizon. *Operations Research*, 21:1071–1088, 1973.

[52] A. Smith. Privacy-preserving statistical estimation with optimal convergence rates. In *Proceedings of the Fourty-Third Annual ACM Symposium on the Theory of Computing*, pages 813–822, 2011.

[53] R. Soosahabi, M. Naraghi-Pour, D. Perkins, and M. A. Bayoumi. Optimal probabilistic encryption for secure detection in wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, 9(3):375–385, 2014.

[54] F. Sultanem. Using appliance signatures for monitoring residential loads at meter panel level. *IEEE Transactions on Power Delivery*, 6(4):1380–1385, 1991.

[55] 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*, 31(7):1331–1341, 2013.

[56] E. Tekin. The Gaussian multiple access wire-tap channel: Wireless secrecy and cooperative jamming. In *Proceedings of ITA 2007*, pages 404–413, 2007.

[57] J. N. Tsitsiklis. Decentralized detection. In *Proceedings of Advances in Statistical Signal Processing*, pages 297–344, 1993.

[58] T. van Erven and P. Harremoës. Rényi divergence and Kullback-Leibler divergence. *IEEE Transactions on Information Theory*, 60(7):3797–3820, 2014.

[59] H. L. van Trees. *Detection, Estimation, and Modulation Theory, Part I*. Wiley-Interscience, 2001.

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

[61] P. K. Varshney. *Distributed Detection and Data Fusion*. Springer-Verlag New York, Inc., 1996.

[62] E. K. Wang, Y. Ye, X. Xu, S. M. Yiu, L. C. K. Hui, and K. P. Chow. Security issues and challenges for cyber physical system. In *Proceedings of GreenCom-CPSCom 2010*, pages 733–738, 2010.

[63] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8): 1355–1387, 1975.

[64] L. Yang, X. Chen, J. Zhang, and H. V. Poor. Optimal privacy-preserving energy management for smart meters. In *Proceedings of INFOCOM 2014*, pages 513–521, 2014.

[65] J. Yao and P. Venkitasubramaniam. On the privacy-cost tradeoff of an in-home power storage mechanism. In *Proceedings of Allerton 2013*, pages 115–122, 2013.

[66] J. Yao and P. Venkitasubramaniam. The privacy analysis of battery control mechanisms in demand response: Revealing state approach and rate distortion bounds. In *Proceedings of CDC 2014*, pages 1377–1382, 2014.

[67] Y. You, Z. Li, and T. J. Oechtering. An optimal privacy-enhancing and cost-efficient energy management strategy. Submitted to WIFS 2017.