July 2020

INFORMATION-THEORETIC LIMITS ON STATISTICAL MATCHING WITH APPLICATIONS TO PRIVACY

Nazanin Takbiri

INFORMATION-THEORETIC LIMITS ON STATISTICAL MATCHING WITH APPLICATIONS TO PRIVACY

A Dissertation Presented

by

NAZANIN TAKBIRI

Submitted to the Graduate School of the
University of Massachusetts Amherst in partial fulfillment
of the requirements for the degree of

DOCTOR OF PHILOSOPHY

May 2020

Electrical and Computer Engineering

INFORMATION-THEORETIC LIMITS ON STATISTICAL MATCHING WITH APPLICATIONS TO PRIVACY

A Dissertation Presented

by

NAZANIN TAKBIRI

Approved as to style and content by:

Hossein Pishro-Nik, Chair

Dennis L. Goeckel, Member

Amir Houmansadr, Member

Marco F. Duarte, Member

Christopher V. Hollot, Department Chair
Electrical and Computer Engineering

DEDICATION

To my mother, to whom I owe everything.

ACKNOWLEDGMENTS

First and foremost, I would like to express my sincere gratitude to my thesis advisor, Prof. Hossein Pishro-Nik, for his constant advice and support at every stage of my Ph.D. program. I am deeply thankful for his unwavering patience and generosity in teaching me the art of research and scientific writing. I would like to thank him for letting me have the most pleasant time during my Ph.D., without any pressure or stress, yet filled by enormous motivations and encouragement. I would like to thank him for always believing in me, and pushing me to go further than I ever thought I could go.

Furthermore, I am extremely grateful to Prof. Dennis L. Goeckel who could as well be my second advisor and has contributed to my learning enormously. I would like to thank him for his invaluable motivation, enthusiasm, support, and immense knowledge that accompanied me throughout my whole graduate program at the University of Massachusetts Amherst. He kindly treated me as one of his students, and his office's door was always open to me. He never said no when I asked for help, which I did in many occasions. I have benefited tremendously from his care, expertise, guidance, and the numerous opportunities he has created for me.

I would like to thank Prof. Amir Houmansadr for his brilliant ideas, which helped me to bridge theory and practice. His insight and vision had a central role in this research. I would also like to thank Prof. Marco F. Duarte for his invaluable questions, comments, and feedback on this dissertation. I would also like to thank Prof. Lixin Gao for co-authoring a paper with me. Furthermore, I would like to thank Prof. Patrick Kelly, for supporting me to fulfill my dream of being an instructor at the University of Massachusetts Amherst and for helping me to teach Signal and System course during Spring 2019.

Further, I would like to thank all of my co-authors who have helped me during my research (in alphabetical order): Minting Chen, Bo Guan, Ke Li, Xiaozhe Shao, Virat Shejwalkar, and Ramin Soltani.

My appreciation also extends to Qualcomm Technology, Inc. for offering me an internship opportunity in Summer 2019. I am extremely fortunate that I was part of the amazing "SoC Security" team in Qualcomm Technology, Inc. Their exemplary guidance, encouragements, and supervision throughout the internship program were so exceptional.

From Tehran to UMass, it was too long and scary to be possible without my family's constant love, guidance, sacrifice, and encouragement. I wish to express my sincerest gratitude toward my parents for giving me the most valuable gift that I could ever ask for: to be able to set my mind to whatever I decide to accomplish. I would also deeply thank my lovely siblings, who always stand by my side despite the endless North Atlantic Ocean stands between us by its entirety.

Finally, I would like to thank my colleague, my best friend, and my husband, Ali, who contributed directly and indirectly to every moment of my Bachelor's, Master's, and Ph.D. programs. I would like to thank him for supporting me after every setback, for sitting and listening to my ambiguous math thoughts for hours when I was stuck in my work, listening to my presentations about one hundred times, traveling thousands of miles to attend most of my presentations and criticizing my work by asking insightful questions and giving valuable feedback. Ever since the day we met, regardless of what has been going on in my life, I have always felt to be the luckiest woman to have such a brilliant, caring, and supportive person in my life.

ABSTRACT

INFORMATION-THEORETIC LIMITS ON STATISTICAL MATCHING WITH APPLICATIONS TO PRIVACY

MAY 2020

NAZANIN TAKBIRI

B.Sc., UNIVERSITY OF TEHRAN

M.Sc., BOĞAZIÇI UNIVERSITY

Ph.D., UNIVERSITY OF MASSACHUSETTS AMHERST

Directed by: Professor Hossein Pishro-Nik

Modern applications significantly enhance user experience by adapting to each user's individual condition and/or preferences. While this adaptation can greatly improve a user's experience or be essential for the application to work, the exposure of user data to the application presents a significant privacy threat to the users—even when the traces are anonymized (since the statistical matching of an anonymized trace to prior user behavior can identify a user and their habits). Because of the current and growing algorithmic and computational capabilities of adversaries, provable privacy guarantees as a function of the degree of anonymization and obfuscation of the traces are necessary. This dissertation focuses on deriving the theoretical bounds on the privacy of users in such a scenario. Here we derive the fundamental limits of user privacy when both anonymization and obfuscation-based protection mechanisms are applied to users' time series of data. We investigate the impact of such mechanisms on the trade-off between privacy protection and user utility. In the first part, the requirements on anonymization and obfuscation in the case that data traces are independent between users are obtained. However, the data traces of different users will be dependent in many applications, and an adversary can potentially exploit such. So in the next part, we consider the impact of dependency between user traces on their privacy. In order to do that, we demonstrate that the adversary can readily identify the association graph of the obfuscated and anonymized version of the data, revealing which user data traces are dependent, and then, we demonstrate that the adversary can use this association graph to break user privacy with significantly shorter traces than in the case of independent users. As a result, we show inter-user dependency degrades user privacy. We show that obfuscating data traces independently across users is often insufficient to remedy such leakage. Therefore, we discuss how users can improve privacy by employing joint obfuscation that removes the data dependency. Finally, we discuss how the remapping technique came to our help to improve user utility and how much remapping is leaking to the adversary when the adversary does not have the full prior information.

TABLE OF CONTENTS

Page

CHAPTER

LIST OF TABLES

LIST OF FIGURES

Figure **Page**

CHAPTER 1

INTRODUCTION

1.1 Motivation

A number of emerging systems and applications work by analyzing the data submitted by their users in order to serve them; we call such systems *User-Data Driven* (UDD) services. Examples of UDD services include smart cities, connected vehicles, smart homes, and connected healthcare devices, which have the promise of greatly improving users' lives. Unfortunately, the sheer volume of user data collected by these systems can compromise users' privacy [85]. Even the use of standard Privacy-Protection Mechanisms (PPMs), specifically anonymization of user identities and obfuscation of submitted data, does not guarantee users' privacy, as adversaries are able to use powerful statistical inference techniques to learn sensitive private information of the users [74]. Such privacy threats are a major obstacle to the wide adoption of IoT applications, as demonstrated by prior studies [3, 5, 27, 44, 47, 66, 84, 85, 87, 101, 115, 116, 118, 120, 122].

To illustrate the threat of privacy leakage, consider three popular UDD services: (1) *Health care:* Wearable monitors that constantly track user health variables can be invaluable in assessing individual health trends and responding to emergencies. However, such monitors produce long time-series of user data uniquely matched to the health characteristics of each user; (2) *Smart homes:* Emerging smart-home technologies such as fine-grained power measurement systems can help users and utility providers to address one of the key challenges of the twenty-first century: energy conservation. But the measurements of power by such devices can be mapped to users and reveal their lifestyle habits; and, (3) *Connected vehicles:* The location data provided by connected vehicles promises to greatly improve everyday life by reducing congestion and traffic accidents. However, the matching of such location traces to prior behavior not only allows for user tracking, but also reveals a user's habits. In summary, despite their potential impact on society and their emerging popularity, these UDD services have one thing in common: their utility critically depends on their collection of user data, which puts users' privacy at significant risk.

1.2 Related Works

There are two main approaches to augment privacy in UDD services: *identity perturbation (anonymization)* [18, 33, 45, 71, 74, 96, 102, 103], and *data perturbation (obfuscation)* [10,39,99]. In anonymization techniques, privacy is obtained by concealing the mapping between users and data, and the mapping is changed periodically to thwart statistical inference attacks that try to de-anonymize the anonymized data traces by matching user data to known user profiles. Some approaches employ k-anonymity to keep each user's identity indistinguishable within a group of $k-1$ other users [28,36,50,69,105,133,134]. Other approaches employ users' pseudonyms within areas called mix-zones [8, 34, 81]. Obfuscation mechanisms aim at protecting privacy by perturbing user data, e.g., by adding noise to users' samples of data. For instance, cloaking replaces each user's sample of data with a larger region [15,46,98,117,124,136], while an alternative approach is to use dummy data in the set of possible data of the users [16,54,55,70,91]. In [123], a mechanism of obfuscation was introduced where the answer was changed randomly with some small probability. Here we consider the fundamental limits of a similar obfuscation technique for providing privacy in the long time series of emerging applications.

The anonymization and obfuscation mechanisms improve user privacy at the cost of user utility. The anonymization mechanism works by frequently changing the pseudonym mappings of users to reduce the length of time series that can be exploited by statistical analysis. However, this frequent change may also decrease the usability by concealing the temporal relation between a user's sample of data, which may be critical in the utility of some systems, e.g., a dining recommendation system that makes suggestions based on the dining history of its users. On the other hand, obfuscation mechanisms work by adding noise to users' collected data, e.g., location information. The added noise may degrade the utility of UDD applications. Thus, choosing the right level of the privacy-protection mechanism is an important question, and understanding what levels of anonymization and obfuscation can provide theoretical guarantees of privacy is of interest.

Numerous researchers have put forward ideas for quantifying privacy-protection. Shokri et al. [96, 97] define the expected estimation error of the adversary as a metric to evaluate PPMs. Ma et al. [71] use uncertainty about users' information to quantify user privacy in vehicular networks. To defeat localization attacks and achieve privacy at the same time, Shokri et al. [99] proposed a method which finds optimal PPM for a Location Based Service (LBS) given service quality constraints. In [60] and [76], privacy leakage of data sharing and interdependent privacy risks are quantified, respectively. A similar idea is proposed in [132] where the quantification model is based on the Bayes conditional risk. Previously, mutual information has been used as a privacy metric in a number of settings, [11, 19, 64, 65, 88, 89, 127]. However, the framework and problem formulation for our setting (Internet of Things (IoT) privacy) are quite different from those encountered in previous works. More specifically, the IoT privacy problem we consider here is based on a large set of time-series data that belongs to different users with different statistical patterns that has gone through a privacy-preserving mechanism, and the adversary is aiming at de-anonymizing and de-obfuscating the data.

The discussed studies demonstrate the growing importance of privacy. What is missing from the current literature is a solid theoretical framework for privacy that is general enough to encompass various privacy-preserving methods in the literature. Such a framework will allow us to achieve provable privacy guarantees, obtain fundamental trade-offs between privacy and performance, and provide analytical tools to optimally achieve provable privacy.

1.3 Contributions

- **Privacy of Independent Users Against Statistical Matching (Chapter 2):**

  In this chapter, we derive the fundamental limits of user privacy when both anonymization and obfuscation-based protection mechanisms are applied to users' time series of data. We investigate the impact of such mechanisms on the trade-off between privacy protection and user utility in the case that data traces are independent between users. We first study achievability results for the case where the time-series of users are governed by an i.i.d. process. The converse results are proved both for the i.i.d. case as well as the more general Markov chain model. We demonstrate that as the number of users in the network grows, the obfuscation-anonymization plane can be divided into two regions: in the first region, all users have perfect privacy; and, in the second region, no user has privacy.

- **Privacy of Independent Users Against Statistical Matching: Non-Asymptotic Results (Chapter 3)**

  In this chapter, we turn attention to exact performance analysis for a finite number of users and observations. We consider the case where a user is distributed over a discrete set of states according to a probability distribution drawn at random, which we assume is known to the adversary based on his/her analysis of past user behavior. The finite-length traces are then anonymized and obfuscated at a cost in user utility. We analyze the ability of the adversary to correctly identify user data samples as a function of the rate of anonymization and degree of obfuscation, and we arrive at complicated yet readily numerically evaluated expressions. These results allow us to investigate interesting questions left open by the asymptotic nature of previous work.

- **Privacy of Dependent Users Against Statistical Matching(Chapter 4):**

  Chapter 2 has considered the requirements on anonymization and obfuscation for "perfect" user privacy when traces are independent between users. However, in practice users have correlated data traces, as relationships between users establish dependence in their behavior. In this chapter, we demonstrate that such dependency degrades the privacy of PPMs, as the anonymization employed must be significantly increased to preserve perfect privacy, and often no degree of independent obfuscation of the traces can be effective. We also present preliminary results on dependent obfuscation to improve users' privacy.

- **Leveraging Prior Knowledge asymmetries in the Design of IoT Privacy-Preserving Mechanisms (Chapter 5):**

  The Internet of Things (IoT) promises to improve user utility by tuning applications to user behavior, but the revealing of the characteristics of a user's behavior presents a significant privacy risk. Recently, the technique of remapping has been introduced in the privacy literature. Remapping exploits asymmetries in knowledge and/or sophistication between the intended application and the adversary; in particular, the user publishes a more accurate version of their data than they might have otherwise because a sophisticated adversary could obtain that accurate version anyway. We present an information-theoretic analysis of the remapping technique. After introducing a system model, we first demonstrate the mechanism behind the remapping technique. Next, we characterize the loss in privacy when the user lacks knowledge of the accuracy of the adversary's statistical model; this loss in privacy occurs both because the adversary obtains a more accurate view of the user data than expected and because the adversary can exploit the remapping to improve their statistical model more than would have been possible when remapping is not employed. Finally, we introduce a random remapping approach as a countermeasure; in particular, for a given utility, the random remapping approach makes it difficult for the adversary to improve their statistical model.

Finally, in Chapter 6, we present our conclusions and future work.

CHAPTER 2

PRIVACY OF INDEPENDENT USERS AGAINST STATISTICAL MATCHING

2.1 Introduction

Many popular applications use traces of user data to offer various services to their users. However, even if user data is anonymized and obfuscated, a user's privacy can be compromised through the use of statistical matching techniques that match a user trace to prior user behavior. In this chapter, we derive the theoretical bounds on the privacy of users in such a scenario.

Here, we will consider the ability of an adversary to perform statistical analyses on time series and match the series to descriptions of user behavior. In related work, Unnikrishnan [118] provides a comprehensive analysis of the asymptotic (in the length of the time series) optimal matching of time series to source distributions. However, there are several key differences between that analysis and the work here. First, Unnikrishnan [118] looks at the optimal matching tests, but does not consider any privacy metrics as considered in this dissertation, and a significant component of our study is demonstrating that mutual information converges to zero so that we can conclude there is no privacy leakage (hence, "perfect privacy"). Second, the setting of [118] is different, as it does not consider: (a) obfuscation, which is one of the two major protection mechanisms; and (b) sources that are not independent and identically distributed (i.i.d.). Third, the setting of Unnikrishnan [118] assumes a fixed distribution on sources (i.e., classical inference), whereas we assume the existence of general (but possibly unknown) prior distributions for the sources

The work presented in this chapter was published in [106, 107, 109, 111].

(i.e., a Bayesian setting). Finally, we study the fundamental limits in terms of both the number of users and the number of observations, while Unnikrishnan [118] focuses on the case where the number of users is a fixed, finite value.

We derive the fundamental limits of user privacy when both anonymization and obfuscation-based protection mechanisms are applied to users' time series of data. We investigate the impact of such mechanisms on the trade-off between privacy protection and user utility in the case that data traces are independent between users.

In this chapter, we consider two models for users' data: i.i.d. and Markov chains. After introducing the general framework in Section 2.2, we consider an i.i.d. model extensively in Section 2.3 and the first half of Section 2.4. We obtain achievability and converse results for the i.i.d. model. The i.i.d. model would apply directly to data that is sampled at a low rate. In addition, understanding the i.i.d. case can also be considered the first step toward understanding the more complicated case where there is dependency, as was done for anonymization-only Location Privacy-Preserving Mechanisms (LPPMs) in [73], and will be done in Section 2.4.3. In particular, in Section 2.4.3, a general Markov chain model is used to model users' data pattern to capture the dependency of the user' data pattern over time. There, we obtain converse results for privacy for this model. In Section 2.5, we provide some discussion about the achievability for the Markov chain case.

2.2 System Model, Definitions, and Metrics

In this chapter, we adopt a similar framework to that employed in [73,106]. The general set up is provided here, and the refinement to the precise models for this chapter will be presented in the following sections. We assume a system with n users with $X_u(k)$ denoting a sample of the data of user u at time k, which we would like to protect from an interested adversary. We consider a strong adversary that has complete statistical knowledge of the users' data patterns based on the previous observations or other resources. In order to secure data privacy of users, both obfuscation and anonymization techniques are used as shown in Figure 2.1. In Figure 2.1, $Z_u(k)$ shows the (reported) sample of the data of user u at time k after applying obfuscation, and $Y_u(k)$ shows the (reported) sample of the data of user u at time k after applying anonymization. The adversary observes only $Y_u(k)$, $k = 1, 2, \cdots, m(n)$, where $m(n)$ is the number of observations of each user before the identities are permuted. The adversary then tries to estimate $X_u(k)$ by using those observations.

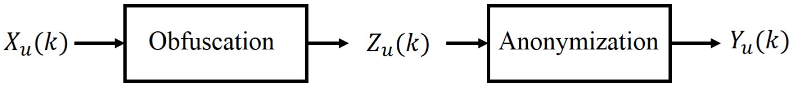


Figure 2.1: Applying obfuscation and anonymization techniques to users' data samples.

Let $\mathbf{X}_u$ be the $m(n) \times 1$ vector containing the samples of the data of user u, and $\mathbf{X}$ be the $m(n) \times n$ matrix with u^{th} column equal to $\mathbf{X}_u$;

$$\mathbf{X}_u = \begin{bmatrix} X_u(1) \\ X_u(2) \\ \vdots \\ X_u(m) \end{bmatrix}, \quad \mathbf{X} = [\mathbf{X}_1, \mathbf{X}_2, \cdots, \mathbf{X}_n].$$

Data Samples Model: We assume there are $r \geq 2$ possible values $(0, 1, \cdots, r-1)$ for each sample of the users' data. In the first part of this chapter (perfect privacy analysis), we assume an i.i.d. model as motivated in Section 2.1. In the second part of this chapter (converse results: no privacy region), the users' datasets are governed by irreducible and aperiodic Markov chains. At any time, $X_u(k)$ is equal to a value in $\{0, 1, \cdots, r-1\}$ according to a user-specific probability distribution. The collection of user distributions, which satisfy some mild regularity conditions discussed below, is known to the adversary, and they employ such to distinguish different users based on statistical matching of those user distributions to traces of user activity of length $m(n)$.

Obfuscation Model: The first step in obtaining privacy is to apply the obfuscation operation in order to perturb the users' data samples. In this chapter, we assume that each user has only limited knowledge of the characteristics of the overall population and thus we employ a simple distributed method in which the samples of the data of each user are reported with error with a certain probability, where that probability itself is generated randomly for each user. In other words, the obfuscated data is obtained by passing the users' data through an r-ary symmetric channel with a random error probability. More precisely, let $\mathbf{Z}_u$ be the vector which contains the obfuscated versions of user u's data samples, and $\mathbf{Z}$ is the collection of $\mathbf{Z}_u$ for all users,

$$\mathbf{Z}_u = \begin{bmatrix} Z_u(1) \\ Z_u(2) \\ \vdots \\ Z_u(m) \end{bmatrix}, \quad \mathbf{Z} = [\mathbf{Z}_1, \mathbf{Z}_2, \cdots, \mathbf{Z}_n] .$$

To create a noisy version of data samples, for each user u, we independently generate a random variable R_u that is uniformly distributed between 0 and a_n, where $a_n \in (0, 1]$. The value of R_u gives the probability that a user's data sample is changed to a different data sample by obfuscation, and a_n is termed the "noise level" of the system. For the case of $r = 2$ where there are two states for users' data (state 0 and state 1), the obfuscated data is obtained by passing users' data through a Binary Symmetric Channel (BSC) with a small error probability [123]. Thus, we can write

$$Z_u(k) = \begin{cases} X_u(k), & \text{with probability } 1 - R_u. \\ 1 - X_u(k), & \text{with probability } R_u. \end{cases}$$

When $r > 2$, for $l \in \{0, 1, \cdots, r-1\}$:

$$\mathbb{P}(Z_u(k) = l | X_u(k) = i) = \begin{cases} 1 - R_u, & \text{for } l = i. \\ \frac{R_u}{r-1}, & \text{for } l \neq i. \end{cases}$$

Note that the effect of the obfuscation is to alter the probability distribution function of each user across the r possibilities in a way that is unknown to the adversary, since it is independent of all past activity of the user, and hence the obfuscation inhibits user identification. For each user, R_u is generated once and is kept constant for the collection of samples of length $m(n)$, thus, providing a very low-weight obfuscation algorithm. We will discuss the extension to the case where R_u is regenerated independently over time in Section 2.5. There, we will also provide a discussion about obfuscation using continuous noise distributions (e.g., Gaussian noise).

Anonymization Model: Anonymization is modeled by a random permutation Π on the set of n users. The user u is assigned the pseudonym $\Pi(u)$. $\mathbf{Y}$ is the anonymized version of $\mathbf{Z}$; thus,

$$\begin{aligned} \mathbf{Y} &= \text{Perm}\left(\mathbf{Z}_1, \mathbf{Z}_2, \cdots, \mathbf{Z}_n; \Pi\right) \\ &= \left[\mathbf{Z}_{\Pi^{-1}(1)}, \mathbf{Z}_{\Pi^{-1}(2)}, \cdots, \mathbf{Z}_{\Pi^{-1}(n)}\right] \\ &= \left[\mathbf{Y}_1, \mathbf{Y}_2, \cdots, \mathbf{Y}_n\right], \end{aligned}$$

where Perm(. , Π) is permutation operation with permutation function Π. As a result, $\mathbf{Y}_u = \mathbf{Z}_{\Pi^{-1}(u)}$ and $\mathbf{Y}_{\Pi(u)} = \mathbf{Z}_u$.

Here we provide a simple example to further elaborate the problem setting. Let us assume there are three users in the setting, $n = 3$, and there exists five possible values for each data point of user u, $r = 5$. Also, let us assume the number of adversary's observations per user is equal to 6, $m = 6$. Now, each user has a data sequence as below:

Users	Data sequences
User 1	$0 \rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 0$
User 2	$1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 0 \rightarrow 1$
User 3	$2 \rightarrow 3 \rightarrow 4 \rightarrow 0 \rightarrow 2 \rightarrow 4$

$$\mathbf{X} = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 0 \\ 4 & 0 & 2 \\ 0 & 1 & 4 \end{bmatrix}.$$

In order to anonymized data, we change the pseudonyms of users. These pseudonyms are determined by the function defined by a random permutation on the user set:

$$\Pi : \{1, 2, 3\} \mapsto \{1, 2, 3\}.$$

Now, assume $\Pi(1) = 2$, $\Pi(2) = 3$, and $\Pi(3) = 1$. Thus, the adversary observes the anonymized version of data $\mathbf{Y}$, so they observe

Pseudonyms	Observed data by the adversary
user 1	$2 \rightarrow 3 \rightarrow 4 \rightarrow 0 \rightarrow 2 \rightarrow 4$
user 2	$0 \rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 0$
user 3	$1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 0 \rightarrow 1$

$$\mathbf{Y} = \begin{bmatrix} 2 & 0 & 1 \\ 3 & 1 & 2 \\ 4 & 2 & 3 \\ 3 & 1 & 2 \\ 0 & 3 & 4 \\ 4 & 0 & 1 \end{bmatrix}.$$

The adversary tries to de-anonymized data based on their observations and the statistical knowledge of the user's behaviour.

Adversary Model: We protect against the strongest reasonable adversary. Through past observations or some other sources, the adversary is assumed to have complete statistical knowledge of the users' patterns; in other words, they know the probability distribution for each user on the set of data samples $\{0, 1, \dots, r-1\}$. As discussed in the model for the data samples, the parameters $\mathbf{p}_u$, $u = 1, 2, \cdots, n$ are drawn independently from a continuous density function, $f_{\mathbf{P}}(\mathbf{p}_u)$, which has support on a subset of a defined hypercube. The density $f_{\mathbf{P}}(\mathbf{p}_u)$ might be unknown to the adversary, as all that is assumed here is that such a density exists, and it will be evident from our results that knowing or not knowing $f_{\mathbf{P}}(\mathbf{p}_u)$ does not change the results asymptotically. Specifically, from the results we will show in Section 2.3, we conclude that user u has perfect privacy even if the adversary knows $f_{\mathbf{P}}(\mathbf{p}_u)$. In addition, in Section 2.4, it is shown that the adversary can recover the true data of user u at time k

without using the specific density function of $f_{\mathbf{P}}(\mathbf{p}_u)$, and as result, users have no privacy even if the adversary does not know $f_{\mathbf{P}}(\mathbf{p}_u)$.

The adversary also knows the value of noise level a_n as it is a design parameter. However, the adversary does not know the realization of the random permutation Π or the realizations of the random variables R_u, as these are independent of the past behavior of the users. It is critical to note that we assume the adversary does not have any auxiliary information or side information about users' data.

In [73], perfect privacy is defined as follows:

Definition 1. User u has *perfect privacy* at time k, if and only if

$$\lim_{n\to\infty} \mathbb{I}\left(X_u(k);\mathbf{Y}\right) = 0,$$

where $\mathbb{I}(X;Y)$ denotes the mutual information between random variables (vectors) X and Y.

In this chapter, we also consider the situation in which there is no privacy.

Definition 2. For an algorithm for the adversary that tries to estimate the actual data point of user u at time k, define the error probability as

$$\mathbb{P}_e(u,k) = \mathbb{P}\left(\widetilde{X_u(k)} \neq X_u(k)\right),$$

where $X_u(k)$ is the actual data point of user u at time k, $\widetilde{X_u(k)}$ is the adversary's estimated data point of user u at time k. Now, define $\mathcal{E}$ as the set of all possible adversary's estimators. Then, user u has *no privacy* at time k, if and only if,

$$\mathbb{P}_e^*(u,k) = \lim_{n\to\infty} \inf_{\mathcal{E}} \mathbb{P}\left(\widetilde{X_u(k)} \neq X_u(k)\right) \to 0.$$

Hence, a user no privacy at time k if there exists an algorithm for the adversary to estimate $X_u(k)$ with diminishing error probability as n goes to infinity.

Discussion 1: Both of the privacy definitions given above (perfect privacy and no privacy) are asymptotic in the number of users ($n \to \infty$), which allows us to find clean analytical results for the fundamental limits. Moreover, in many IoT applications, such as ride sharing and dining recommendation applications, the number of users is large.

Notation: Note that the sample of data of user u at time k after applying obfuscation ($Z_u(k)$) and the sample of data of user u at time k after applying anonymization ($Y_u(k)$) depend on the number of users in the network (n), while the actual sample of data of user u at time k is independent of the number of users (n). Despite the dependency in the former cases, we omit this subscript (n) on $\left(Z_u^{(n)}(k), Y_u^{(n)}(k)\right)$ to avoid confusion and make the notation consistent.

Notation: Throughout the chapter, $X_n \xrightarrow{d} X$ denotes convergence in distribution. Also, We use $\mathbb{P}\left(X = x \middle| Y = y\right)$ for the conditional probability of $X = x$ given $Y = y$. When we write $\mathbb{P}\left(X = x \middle| Y\right)$, we are referring to a random variable that is defined as a function of Y.

2.3 Perfect Privacy Analysis: I.I.D. Case

2.3.1 Two-State i.i.d. Model

We first consider the two-state case ($r = 2$) which captures the salient aspects of the problem. For the two-state case, the sample of the data of user u at any time is a Bernoulli random variable with parameter p_u, which is the probability of user u having data sample 1. Thus,

$$X_u(k) \sim \text{Bernoulli}\left(p_u\right).$$

Per Section 2.2, the parameters p_u, $u = 1, 2, \cdots, n$ are drawn independently from a continuous density function, $f_P(p_u)$, on the $(0, 1)$ interval. We assume there are $\delta_1, \delta_2 > 0$ such that:[1]

[1] The condition $\delta_1 < f_P(p_u) < \delta_2$ is not actually necessary for the results and can be relaxed; however, we keep it here to avoid unnecessary technicalities.

$$\begin{cases} \delta_1 < f_P(p_u) < \delta_2, & p_u \in (0,1). \\ f_P(p_u) = 0, & p_u \notin (0,1). \end{cases}$$

The adversary knows the values of p_u, $u = 1, 2, \cdots, n$ and uses this knowledge to identify users. We will use capital letters (i.e., P_u) when we are referring to the random variable, and use lower case (i.e., p_u) to refer to the realization of P_u.

In addition, since the user data ($X_u(k)$) are i.i.d. and have a Bernoulli distribution, the obfuscated data ($Z_u(k)$) are also i.i.d. with a Bernoulli distribution. Specifically,

$$Z_u(k) \sim \text{Bernoulli}\left(Q_u\right),$$

where

$$\begin{aligned} Q_u &= P_u(1 - R_u) + (1 - P_u)R_u \\ &= P_u + \left(1 - 2P_u\right)R_u, \end{aligned}$$

and recall that R_u is the probability that user u's data sample is altered at any time. For convenience, define a vector where element Q_u is the probability that an obfuscated data sample of user u is equal to one, and

$$\mathbf{Q} = \left[Q_1, Q_2, \cdots, Q_n\right].$$

Thus, a vector containing the permutation of those probabilities after anonymization is given by:

$$\begin{aligned} \mathbf{W} &= \text{Perm}\left(Q_1, Q_2, \cdots, Q_n; \Pi\right) \\ &= \left[Q_{\Pi^{-1}(1)}, Q_{\Pi^{-1}(2)}, \cdots, Q_{\Pi^{-1}(n)}\right] \\ &= \left[W_1, W_2, \cdots, W_n\right], \end{aligned}$$

where $W_u = Q_{\Pi^{-1}(u)}$ and $W_{\Pi(u)} = Q_u$. As a result, for $u = 1, 2, ..., n$, the distribution of the data symbols for the user with pseudonym u is given by:

$$Y_u(k) \sim \text{Bernoulli}\,(W_u) \sim \text{Bernoulli}\left(Q_{\Pi^{-1}(u)}\right).$$

The following theorem states that if the amount of noise level (a_n) is significantly larger than $\frac{1}{n}$ in this two-state model, then all users have perfect privacy independent of the value of $m(n)$.

Theorem 1. For the above two-state model, if $\mathbf{Z}$ is the obfuscated version of $\mathbf{X}$, and $\mathbf{Y}$ is the anonymized version of $\mathbf{Z}$ as defined above, and

- $m = m(n)$ is arbitrary;
- $R_u \sim \text{Uniform}[0, a_n]$, where $a_n \triangleq \Omega\left(c' n^{-(1-\beta)}\right)$ for any $c' > 0$ and $0 < \beta < 1$;

then, user 1 has perfect privacy.

The proof of Theorem 1 will be provided for the case $0 \leq p_1 < \frac{1}{2}$, as the proof for the case $\frac{1}{2} \leq p_1 \leq 1$ is analogous and is thus omitted.

Intuition behind the Proof of Theorem 1:

Since $m(n)$ is arbitrary, the adversary is able to estimate very accurately (in the limit, perfectly) the distribution from which each data sequence $\mathbf{Y}_u$, $u = 1, 2, \cdots, n$ is drawn; that is, the adversary is able to accurately estimate the probability W_u, $u = 1, 2, \cdots, n$. Clearly, if there were no obfuscation for each user u, the adversary would then simply look for the l such that p_l is very close to W_u and set $\widetilde{X_l(k)} = Y_u(k)$, resulting in no privacy for any user.

We want to make certain that the adversary obtains no information about $X_1(k)$, the sample of data of user 1 at time k. To do such, we will establish that there are a large number of users whom have a probability p_u that when obfuscated could have resulted in a probability consistent with p_1. Consider asking whether another probability p_2 is sufficiently close enough to be confused with p_1 after obfuscation; in particular, we will look for p_2 such that, even if the adversary is given the obfuscated probabilities $W_{\Pi(1)}$ and $W_{\Pi(2)}$, they cannot associate these probabilities with p_1 and p_2. This requires that the distributions Q_1 and Q_2 of the obfuscated data of user 1 and user 2 have significant overlap; we explore this next.

Recall that $Q_u = P_u+(1-2P_u)R_u$, and $R_u \sim \text{Uniform}[0, a_n]$. Thus, we know $Q_u|P_u = p_u$ has a uniform distribution with length $(1-2p_u)a_n$. Specifically,

$$Q_u \Big| P_u = p_u \sim \text{Uniform}\left[p_u, p_u + (1-2p_u)a_n\right].$$

Figure 2.2 shows the distribution of Q_u given $P_u = p_u$.

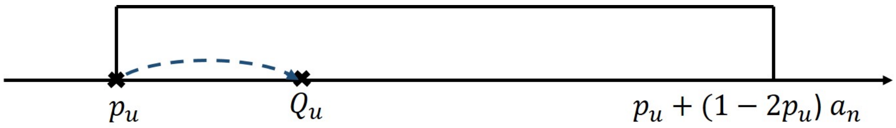


Figure 2.2: Distribution of Q_u given $P_u = p_u$.

Consider two cases: In the first case, the support of the distributions $Q_1 \big| P_1 = p_1$ and $Q_2 \big| P_2 = p_2$ are small relative to the difference between p_1 and p_2 (Figure 2.3); in this case, given the probabilities $W_{\Pi(1)}$ and $W_{\Pi(2)}$ of the anonymized data sequences, the adversary can associate those with p_1 and p_2 without error. In the second case, the support of the distributions $Q_1 \big| P_1 = p_1$ and $Q_2 \big| P_2 = p_2$ is large relative to the difference between p_1 and p_2 (Figure 2.4), so it is difficult for the adversary to associate the probabilities $W_{\Pi(1)}$ and $W_{\Pi(2)}$ of the anonymized data sequences with p_1 and p_2. In particular, if $W_{\Pi(1)}$ and $W_{\Pi(2)}$ fall into the overlap of the support of Q_1 and Q_2, we will show the adversary can only guess randomly how to de-anonymize the data. Thus, if the ratio of the support of the distributions to $\big|p_1 - p_2\big|$ goes to infinity, the adversary's posterior probability for each user converges to $\frac{1}{2}$, thus, implying no information leakage on the user identities. More generally, if we can guarantee that there will be a large set of users with p_u's very close to p_1 compared to the support of $Q_1 \big| P_1 = p_1$, we will be able to obtain perfect privacy as demonstrated rigorously below.

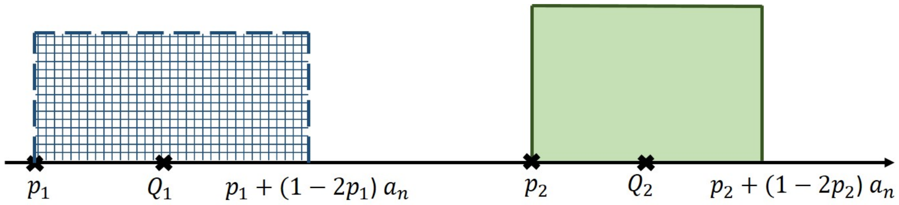


Figure 2.3: Case 1: The support of the distributions is small relative to the difference between p_1 and p_2.

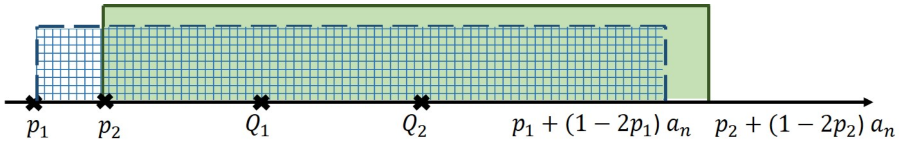


Figure 2.4: Case 2: The support of the distributions is large relative to the difference between p_1 and p_2.

Given this intuition, the formal proof proceeds as follows. Given p_1, we define a set $J^{(n)}$ of users whose parameter p_u of their data distributions is sufficiently close to p_1 (Figure 2.4; case 2), so that it is likely that Q_1 and Q_u cannot be readily associated with p_1 and p_u.

The purpose of Lemmas 1, 2, and 3 is to show that, from the adversary's perspective, the users in set $J^{(n)}$ are indistinguishable. More specifically, the goal is to show that the obfuscated data corresponding to each of these users could have been generated by any other users in $J^{(n)}$ in an equally likely manner. To show this, Lemma 1 employs the fact that, if the observed values of N uniformly distributed random variables (N is size of set $J^{(n)}$) are within the intersection of their ranges, it is impossible to infer any information about the matching between the observed values and the distributions. That is, all possible $N!$ matchings are equally likely. Lemmas 2 and 3 leverage Lemma 1 to show that even if the adversary is given a set that includes all of the pseudonyms of the users in set $J^{(n)}$ (i.e., $\Pi(J^{(n)}) \triangleq \left\{\Pi^{-1}(u) \in J^{(n)}\right\}$) they still will not be able to infer any information about the matching of each specific user in set $J^{(n)}$ and his pseudonym. Then Lemma 5 uses the above fact to show that the mutual information between the data set of user 1 at time k and the observed data sets of the adversary converges to zero as $n \to \infty$.

Proof of Theorem 1:

Proof. Note, per Lemma 6 of Appendix 2.8.1, it is sufficient to establish the results on a sequence of sets with high probability. That is, we can condition on high-probability events.

Now, as shown in Figure 2.5, define the critical set $J^{(n)}$ with size $N^{(n)} = \left|J^{(n)}\right|$ for $0 \leq p_1 < \frac{1}{2}$ as follows:

$$J^{(n)} = \left\{u \in \{1, 2, \ldots, n\} : p_1 \leq P_u \leq p_1 + \epsilon_n; p_1 + \epsilon_n \leq Q_u \leq p_1 + (1 - 2p_1)a_n\right\},$$

where $\epsilon_n \triangleq \frac{1}{n^{1-\frac{\beta}{2}}}$, $a_n = c'n^{-(1-\beta)}$, and β is defined in the statement of Theorem 1.

Note for large enough n, if $0 \leq p_1 < \frac{1}{2}$, we have $0 \leq p_u < \frac{1}{2}$. As a result,

$$Q_u \middle| P_u = p_u \sim \text{Uniform}\left(p_u, p_u + (1 - 2p_u)a_n\right).$$

We can prove that with high probability, $1 \in J^{(n)}$ for large enough n, as follows. First, Note that

$$Q_1 \middle| P_1 = p_1 \sim \text{Uniform}\left(p_1, p_1 + (1 - 2p_1)a_n\right).$$

Now, according to Figure 2.6,

$$\begin{aligned} \mathbb{P}\left(1 \in J^{(n)}\right) &= 1 - \frac{\epsilon_n}{(1 - 2p_1)\, a_n} \\ &= 1 - \frac{1}{(1 - 2p_1)\, c'n^{\frac{\beta}{2}}}, \end{aligned}$$

thus, for any $c' > 0$ and large enough n,

$$\mathbb{P}\left(1 \in J^{(n)}\right) \to 1.$$

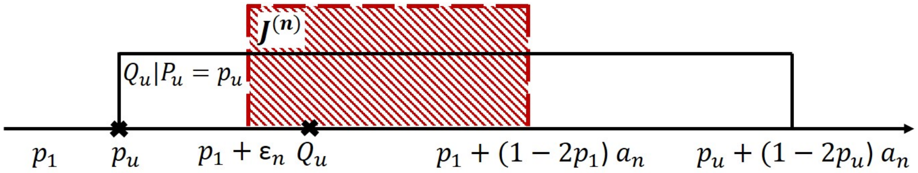


Figure 2.5: Range of P_u and Q_u for elements of set $J^{(n)}$ and probability density function of $Q_u \big| P_u = p_u$.

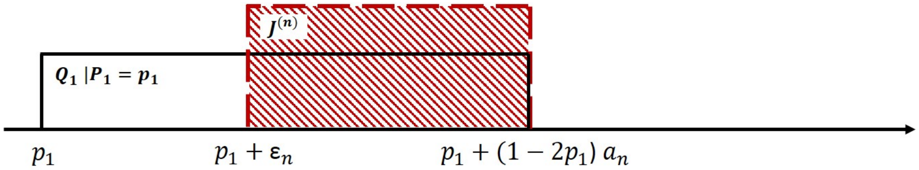


Figure 2.6: Range of P_u and Q_u for elements of set $J^{(n)}$ and probability density function of $Q_1 \big| P_1 = p_1$.

Now in the second step, we define the probability $\mathcal{J}_l^{(n)}$ for any $l \in \Pi(J^{(n)}) = \{\Pi(u) : u \in J^{(n)}\}$ as

$$\mathcal{J}_l^{(n)} = \mathbb{P}\left(\Pi(1) = l \middle| \mathbf{W}, \Pi(J^{(n)})\right).$$

$\mathcal{J}_l^{(n)}$ is the conditional probability that $\Pi(1) = l$ after perfectly observing the values of the permuted version of obfuscated probabilities ($\mathbf{W}$) and set including all of the pseudonyms of the users in set $J^{(n)}$ $\left(\Pi(J^{(n)})\right)$. Since $\mathbf{W}$ and $\Pi(J^{(n)})$ are random, $\mathcal{J}_l^{(n)}$ is a random variable. However, we will prove shortly that in fact $\mathcal{J}_l^{(n)} = \frac{1}{N^{(n)}}$, for all $l \in \Pi(J^{(n)})$.

Note: Since we are looking from the adversary's point of view, the assumption is that all the values of p_u, $u \in \{1, 2, \cdots, n\}$ are known, so all of the probabilities are conditioned on the values of $P_1 = p_1, P_2 = p_2, \cdots, P_n = p_n$. Thus, to be accurate, we should write

$$\mathcal{J}_l^{(n)} = \mathbb{P}\left(\Pi(1) = l \middle| \mathbf{W}, \Pi(J^{(n)}), P_1, P_2, \cdots, P_n\right).$$

Nevertheless, for simplicity of notation, we often omit the conditioning on $P_1, P_2, \cdots, P_n$.

First, we need a lemma from elementary probability.

Lemma 1. Let N be a positive integer, and let $a_1, a_2, \cdots, a_N$ and $b_1, b_2, \cdots, b_N$ be real numbers such that $a_u \leq b_u$ for all u. Assume that $X_1, X_2, \cdots, X_N$ are independent random variables such that

$$X_u \sim \mathrm{Uniform}[a_u, b_u].$$

Let also $\gamma_1, \gamma_2, \cdots, \gamma_N$ be distinct real numbers such that

$$\gamma_l \in \bigcap_{u=1}^{N} [a_u, b_u] \text{ for all } l \in \{1, 2, .., N\}.$$

Suppose that we know the event E has occurred, meaning that the observed values of X_u's are equal to the set of γ_l's (but with unknown ordering), i.e.,

$$E \quad \equiv \quad \{X_1, X_2, \cdots, X_N\} = \{\gamma_1, \gamma_2, \cdots, \gamma_N\},$$

then

$$\mathbb{P}(X_1 = \gamma_l | E) = \frac{1}{N}.$$

Proof. Lemma 1 is proved in Appendix 2.8.2. □

Using the above lemma, we can state our desired result for $\mathcal{J}_l^{(n)}$.

Lemma 2. For all $l \in \Pi(J^{(n)})$, $\mathcal{J}_l^{(n)} = \frac{1}{N^{(n)}}$.

Proof. We argue that the setting of this lemma is essentially equivalent to the assumptions in Lemma 1. First, remember that

$$\mathcal{J}_l^{(n)} = \mathbb{P}\left(\Pi(1) = l \middle| \mathbf{W}, \Pi(J^{(n)})\right).$$

Note that $Q_u = P_u + (1 - 2P_u)R_u$, and since R_u is uniformly distributed, Q_u conditioned on P_u is also uniformly distributed in the appropriate intervals. Moreover, since $W_u =$

$Q_{\Pi^{-1}(u)}$, we conclude W_u is also uniformly distributed. So, looking at the definition of $\mathcal{J}_l^{(n)}$, we can say the following: given the values of the uniformly distributed random variables Q_u, we would like to know which one of the values in $\mathbf{W}$ is the actual value of $Q_l = W_{\Pi(1)}$, i.e., is $\Pi(1) = l$? This is equivalent to the setting of Lemma 1 as described further below.

Note that since $1 \in J^{(n)}$, $\Pi(1) \in \Pi(J^{(n)})$. Therefore, when searching for the value of $\Pi(1)$, it is sufficient to look inside set $\Pi(J^{(n)})$. Therefore, instead of looking among all the values of W_l, it is sufficient to look at W_l for $l \in \Pi(J^{(n)})$. Let us show these values by $\mathbf{W}_\Pi = \{w_1, w_2, \cdots, w_{N^{(n)}}\}$, so,

$$\mathcal{J}_l^{(n)} = \mathbb{P}\left(\Pi(1) = l \middle| \mathbf{W}_\Pi, \Pi(J^{(n)})\right).$$

Thus, we have the following scenario: $Q_u, u \in J^{(n)}$ are independent random variables, and

$$Q_u \middle| P_u = p_u \sim \text{Uniform}[p_u, p_u + (1 - 2p_u)a_n].$$

Also, $w_1, w_2, \cdots, w_{N^{(n)}}$ are the observed values of Q_u with unknown ordering (unknown mapping Π). We also know from the definition of set $J^{(n)}$ that

$$P_u \le p_1 + \epsilon_n \le Q_u,$$

$$Q_u \le p_1(1 - 2a_n) + a_n \le P_u(1 - 2a_n) + a_n,$$

so, we can conclude

$$w_l \in \bigcap_{u=1}^{N^{(n)}} [p_u, p_u + (1 - 2p_u)a_n] \text{ for all } l \in \{1, 2, .., N^{(n)}\}.$$

We know the event E has occurred, meaning that the observed values of Q_u's are equal to set of w_l's (but with unknown ordering), i.e.,

$$E \equiv \{Q_u, u \in J^{(n)}\} = \{w_1, w_2, \cdots, w_{N^{(n)}}\}.$$

Then, according to Lemma 1,

$$\mathbb{P}\left(Q_1 = w_l | E, P_1, P_2, \cdots, P_n\right) = \frac{1}{N^{(n)}}.$$

Note that there is a subtle difference between this lemma and Lemma 1. Here $N^{(n)}$ is a random variable while N is a fixed number in Lemma 1. Nevertheless, since the assertion holds for every fixed N, it also holds for the case where N is a random variable. Now, note that

$$\begin{aligned}\mathbb{P}\left(Q_1 = w_l | E, P_1, P_2, \cdots, P_n\right) &= \mathbb{P}\left(\Pi(1) = l \middle| E, P_1, P_2, \cdots, P_n\right)\\ &= \mathbb{P}\left(\Pi(1) = l \middle| \mathbf{W}_\Pi, \Pi(J^{(n)}), P_1, P_2, \cdots, P_n\right)\\ &= \mathcal{J}_l^{(n)}.\end{aligned}$$

Thus, we can conclude

$$\mathcal{J}_l^{(n)} = \frac{1}{N^{(n)}}.$$

□

In the third step, we define $\widetilde{\mathcal{J}_l^{(n)}}$ for any $l \in \Pi(J^{(n)})$ as

$$\widetilde{\mathcal{J}_l^{(n)}} = \mathbb{P}\left(\Pi(1) = l \middle| \mathbf{Y}, \Pi(J^{(n)})\right).$$

$\widetilde{\mathcal{J}_l^{(n)}}$ is the conditional probability that $\Pi(1) = l$ after observing the values of the anonymized version of the obfuscated samples of the users' data ($\mathbf{Y}$) and the aggregate set including all the pseudonyms of the users in set $J^{(n)}$ (i.e., $\Pi(J^{(n)}) \triangleq \left\{\Pi^{-1}(l) \in J^{(n)}\right\}$). Since $\mathbf{Y}$ and $\Pi(J^{(n)})$ are random, $\widetilde{\mathcal{J}_l^{(n)}}$ is a random variable. Now, in the following lemma, we will prove $\widetilde{\mathcal{J}_l^{(n)}} = \frac{1}{N^{(n)}}$, for all $l \in \Pi(J^{(n)})$ by using Lemma 3.

Note in the following lemma, we want to show that even if the adversary is given a set including all of the pseudonyms of the users in set $J^{(n)}$, they cannot match each specific user in set $J^{(n)}$ and his pseudonym.

Lemma 3. For all $l \in \Pi(J^{(n)})$, $\widetilde{\mathcal{J}_l^{(n)}} = \frac{1}{N^{(n)}}$.

Proof. First, note that

$$\widetilde{\mathcal{J}_l^{(n)}} = \sum_{\text{for all } \mathbf{w}} \mathbb{P}\left(\Pi(1) = l \middle| \mathbf{Y}, \Pi\left(J^{(n)}\right), \mathbf{W} = \mathbf{w}\right) \mathbb{P}\left(\mathbf{W} = \mathbf{w} \middle| \mathbf{Y}, \Pi\left(J^{(n)}\right)\right).$$

Also, we note that given $\mathbf{V}$, $\Pi(J^{(n)})$, and $\mathbf{Y}$ are independent. Intuitively, this is because when observing $\mathbf{Y}$, any information regarding $\Pi(J^{(n)})$ is leaked through estimating $\mathbf{V}$. This can be rigorously proved similar to the proof of [73, Lemma 1]. We can state this fact as

$$\mathbb{P}\left(Y_u(k) \,\middle|\, W_u = w_u, \Pi(J^{(n)})\right) = \mathbb{P}\left(Y_u(k) \,\middle|\, W_u = w_u\right) = w_u.$$

The right and left hand sides of the above equation are given by $\text{Bernoulli}(w_u)$ distributions. As a result,

$$\widetilde{\mathcal{J}_l^{(n)}} = \sum_{\text{for all } \mathbf{w}} \mathbb{P}\left(\Pi(1) = l \middle| \Pi(J^{(n)}), \mathbf{W} = \mathbf{w}\right) \mathbb{P}\left(\mathbf{W} = \mathbf{w} \middle| \mathbf{Y}, \Pi\left(J^{(n)}\right)\right).$$

Note $\mathcal{J}_l^{(n)} = \mathbb{P}\left(\Pi(1) = l \middle| \Pi(J^{(n)}), \mathbf{W}\right)$, so

$$\begin{aligned}
\widetilde{\mathcal{J}_l^{(n)}} &= \sum_{\text{for all } \mathbf{w}} \mathcal{J}_l^{(n)} \mathbb{P}\left(\mathbf{W} = \mathbf{w} \middle| \mathbf{Y}, \Pi\left(J^{(n)}\right)\right) \\
&= \frac{1}{N^{(n)}} \sum_{\text{for all } \mathbf{w}} \mathbb{P}\left(\mathbf{W} = \mathbf{w} \middle| \mathbf{Y}, \Pi\left(J^{(n)}\right)\right) \\
&= \frac{1}{N^{(n)}}.
\end{aligned}$$

□

To show that no information is leaked, we need to show that the size of set $J^{(n)}$ goes to infinity.

Lemma 4. If $N^{(n)} \triangleq |J^{(n)}|$, then $N^{(n)} \to \infty$ with high probability as $n \to \infty$. More specifically, there exists $\lambda > 0$ such that

$$\mathbb{P}\left(N^{(n)} > \frac{\lambda}{2} n^{\frac{\beta}{2}}\right) \to 1.$$

Proof. Lemma 4 is proved in Appendix 2.8.3. □

In the final step, we define $\widehat{\mathcal{J}_l^{(n)}}$ for any $l \in \Pi(J^{(n)})$ as

$$\widehat{\mathcal{J}_l^{(n)}} = \mathbb{P}\left(X_1(k) = 1 \middle| \mathbf{Y}, \Pi(J^{(n)})\right).$$

$\widehat{\mathcal{J}_l^{(n)}}$ is the conditional probability that $X_1(k) = 1$ after observing the values of the anonymized version of the obfuscated samples of the users' data ($\mathbf{Y}$) and the aggregate set including all of the pseudonyms of the users in set $J^{(n)}$ ($\Pi(J^{(n)})$). $\widehat{\mathcal{J}_l^{(n)}}$ is a random variable because $\mathbf{Y}$ and $\Pi(J^{(n)})$ are random. Now, in the following lemma, we will prove $\widehat{\mathcal{J}_l^{(n)}}$ converges in distribution to p_1.

Note that this is the probability from the adversary's point of view. That is, given that the adversary has observed $\mathbf{Y}$ as well as the extra information $\Pi(J^{(n)})$, what can they infer about $X_1(k)$?

Lemma 5. For all $l \in \Pi(J^{(n)})$, $\widehat{\mathcal{J}_l^{(n)}} \xrightarrow{d} p_1$.

Proof. We know

$$\widehat{\mathcal{J}_l^{(n)}} = \sum_{l \in \Pi(J^{(n)})} \mathbb{P}\left(X_1(k) = 1 \middle| \Pi(1) = l, \mathbf{Y}, \Pi(J^{(n)})\right) \mathbb{P}\left(\Pi(1) = l \middle| \mathbf{Y}, \Pi(J^{(n)})\right),$$

and according to the definition $\widetilde{\mathcal{J}_l^{(n)}} = P\left(\Pi(1) = l \middle| \mathbf{Y}, \Pi(J^{(n)})\right)$, we have

$$\widehat{\mathcal{J}_l^{(n)}} = \sum_{l \in \Pi(J^{(n)})} \mathbb{P}\left(X_1(k) = 1 \middle| \Pi(1) = l, \mathbf{Y}, \Pi(J^{(n)})\right) \widetilde{\mathcal{J}_l^{(n)}}$$

$$= \frac{1}{N^{(n)}} \sum_{l \in \Pi(J^{(n)})} \mathbb{P}\left(X_1(k) = 1 \middle| \Pi(1) = l, \mathbf{Y}, \Pi(J^{(n)}) \right).$$

We now claim that

$$\mathbb{P}\left(X_1(k) = 1 \middle| \Pi(1) = l, \mathbf{Y}, \Pi(J^{(n)}) \right) = p_1 + o(1).$$

The reasoning goes as follows. Given $\Pi(1) = l$ and knowing $\mathbf{Y}$, we know that

$$Y_{\Pi(1)}(k) = Z_1(k) = \begin{cases} X_1(k), & \text{with probability } 1 - R_1. \\ 1 - X_1(k), & \text{with probability } R_1. \end{cases}$$

Thus, given $Y_l(k) = 1$, Bayes' rule yields:

$$\begin{aligned} \mathbb{P}\left(X_1(k) = 1 \middle| \Pi(1) = l, \mathbf{Y}, \Pi(J^{(n)}) \right) &= (1 - R_1) \frac{\mathbb{P}(X_1(k) = 1)}{\mathbb{P}(Y_{\Pi(1)}(k) = 1)} \\ &= (1 - R_1) \frac{p_1}{p_1(1 - R_1) + (1 - p_1)R_1} \\ &= 1 - o(1), \end{aligned}$$

and similarly, given $Y_l(k) = 0$,

$$\begin{aligned} \mathbb{P}\left(X_1(k) = 1 \middle| \Pi(1) = l, \mathbf{Y}, \Pi(J^{(n)}) \right) &= R_1 \frac{\mathbb{P}(X_1(k) = 1)}{\mathbb{P}(Y_{\Pi(1)}(k) = 0)} \\ &= R_1 \frac{p_1}{p_1 R_1 + (1 - p_1)(R_1 - 1)} \\ &= o(1). \end{aligned}$$

Note that by the independence assumption, the above probabilities do not depend on the other values of $Y_u(k)$ (as we are conditioning on $\Pi(1) = l$). Thus, we can write

$$\widehat{\mathcal{J}_l^{(n)}} = \frac{1}{N^{(n)}} \sum_{l \in \Pi(J^{(n)})} \mathbb{P}\left(X_1(k) = 1 \middle| \Pi(1) = l, \mathbf{Y}, \Pi(J^{(n)}) \right)$$

$$= \frac{1}{N^{(n)}} \sum_{l \in \Pi(J^{(n)}), Y_l(k)=1} (1 - o(1)) + \frac{1}{N^{(n)}} \sum_{l \in \Pi(J^{(n)}), Y_l(k)=0} o(1).$$

First, note that since $\left|\left\{l \in \Pi(J^{(n)}), Y_l(k) = 0\right\}\right| \leq N^{(n)}$, the second term above converges to zero, thus,

$$\widehat{\mathcal{J}_l^{(n)}} \to \frac{\left|\left\{l \in \Pi(J^{(n)}), Y_{\Pi(1)}(k) = 1\right\}\right|}{N^{(n)}}.$$

Since for all $l \in \Pi(J^{(n)})$, $Y_l(k) \sim \text{Bernoulli}\,(p_1 + o(1))$, by a simple application of Chebyshev's inequality, we can conclude $\widehat{\mathcal{J}_l^{(n)}} \to p_1$. Appendix 2.8.4 provides the detail. □

As a result,

$$X_1(k)|\mathbf{Y}, \Pi(J^{(n)}) \to \text{Bernoulli}(p_1),$$

thus,

$$H\left(X_1(k)\middle|\mathbf{Y}, \Pi(J^{(n)})\right) \to H\left(X_1(k)\right).$$

Since conditioning reduces entropy,

$$H\left(X_1(k)\middle|\mathbf{Y}, \Pi(J^{(n)})\right) \leq H\left(X_1(k)\middle|\mathbf{Y}\right),$$

and as a result,

$$\lim_{n\to\infty} H\left(X_1(k)\right) - H\left(X_1(k)\middle|\mathbf{Y}\right) \leq 0,$$

and

$$\lim_{n\to\infty} \mathbb{I}\left(X_1(k); \mathbf{Y}\right) \leq 0.$$

By knowing that $\mathbb{I}\left(X_1(k); \mathbf{Y}\right)$ cannot take any negative value, we can conclude that

$$\mathbb{I}\left(X_1(k); \mathbf{Y}\right) \to 0.$$

□

2.3.2 r-State i.i.d. Model

Now, assume users' data samples can have r possibilities $(0, 1, \cdots, r-1)$, and $p_u(i)$ shows the probability of user u having data sample i. We define the vector $\mathbf{p}_u$ and the matrix $\mathbf{p}$ as

$$\mathbf{p}_u = \begin{bmatrix} p_u(1) \\ p_u(2) \\ \vdots \\ p_u(r-1) \end{bmatrix}, \quad \mathbf{p} = \left[\mathbf{p}_1, \mathbf{p}_2, \cdots, \mathbf{p}_n\right].$$

We assume $p_u(i)$'s are drawn independently from some continuous density function, $f_{\mathbf{P}}(\mathbf{p}_u)$, which has support on a subset of the $(0,1)^{r-1}$ hypercube (Note that the $p_u(i)$'s sum to one, so one of them can be considered as the dependent value and the dimension is $r-1$). In particular, define the range of the distribution as

$$\mathcal{R}_{\mathbf{p}} = \{(x_1, x_2, \cdots, x_{r-1}) \in (0,1)^{r-1} : x_i > 0, x_1 + x_2 + \cdots + x_{r-1} < 1,\ i = 1, 2, \cdots, r-1\}.$$

Figure 2.7 shows the range $\mathcal{R}_{\mathbf{p}}$ for the case where $r = 3$.

Then, we assume there are $\delta_1, \delta_2 > 0$ such that:

$$\begin{cases} \delta_1 < f_{\mathbf{P}}(\mathbf{p}_u) < \delta_2, & \mathbf{p}_u \in \mathcal{R}_{\mathbf{p}}. \\ f_{\mathbf{P}}(\mathbf{p}_u) = 0, & \mathbf{p}_u \notin \mathcal{R}_{\mathbf{p}}. \end{cases}$$

The obfuscation is similar to the two-state case. Specifically, for $l \in \{0, 1, \cdots, r-1\}$, we can write

$$\mathbb{P}(Z_u(k) = l | X_u(k) = i) = \begin{cases} 1 - R_u, & \text{for } l = i. \\ \frac{R_u}{r-1}, & \text{for } l \neq i. \end{cases}$$

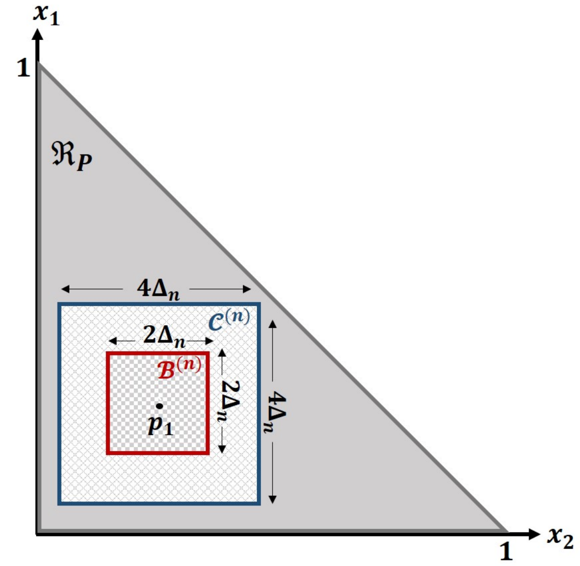


Figure 2.7: $\mathcal{R}_{\mathbf{p}}$ for case $r = 3$.

Theorem 2. For the above r-state model, if $\mathbf{Z}$ is the obfuscated version of $\mathbf{X}$, and $\mathbf{Y}$ is the anonymized version of $\mathbf{Z}$ as defined previously, and

- $m = m(n)$ is arbitrary;
- $R_u \sim \text{Uniform}[0, a_n]$, where $a_n \triangleq \Omega\left(c' n^{-\left(\frac{1}{r-1}-\beta\right)}\right)$ for any $c' > 0$ and $0 < \beta < \frac{1}{r-1}$;

then, user 1 has perfect privacy.

The proof of Theorem 2 is similar to the proof of Theorem 1. The major difference is that instead of the random variables P_u, Q_u, W_u, we need to consider the random vectors $\mathbf{P}_u, \mathbf{Q}_u, \mathbf{W}_u$. Similarly, for user u, we define the vector $\mathbf{Q}_u$ as

$$\mathbf{Q}_u = \begin{bmatrix} Q_u(1) \\ \\ Q_u(2) \\ \\ \vdots \\ \\ Q_u(r-1) \end{bmatrix}.$$

In the r-state case,

$$\begin{aligned} Q_u(i) &= P_u(i)\Big(1 - R_u\Big) + \Big(1 - P_u(i)\Big)\frac{R_u}{r-1} \\ &= P_u(i) + \Big(1 - rP_u(i)\Big)\frac{R_u}{r-1}. \end{aligned}$$

We also need to define the critical set $J^{(n)}$. First, for $i = 0, 1, \cdots, r-1$, define set $J_i^{(n)}$ as follows. If $0 \leq p_1(i) < \frac{1}{r}$, then,

$$\begin{aligned} J_i^{(n)} = \Big\{ & u \in \{1, 2, \ldots, n\} : \\ & p_1(i) \leq P_u(i) \leq p_1(i) + \epsilon_n ; p_1(i) + \epsilon_n \leq Q_u(i) \leq p_1(i) + (1 - rp_1(i))\frac{a_n}{r-1} \Big\}, \end{aligned}$$

where $\epsilon_n \triangleq \frac{1}{n^{\frac{1}{r-1} - \frac{\beta}{2}}}$, $a_n = c' n^{-(\frac{1}{r-1} - \beta)}$, and β is defined in the statement of Theorem 2. We then define the critical set $J^{(n)}$ as:

$$J^{(n)} = \bigcap_{l=0}^{r-1} J_i^{(n)}.$$

We can then repeat the same arguments in the proof of Theorem 1 to complete the proof.

2.4 Converse Results: No Privacy Region

In this section, we prove that if the number of observations by the adversary is larger than its critical value and the noise level is less than its critical value, then the adversary can find an algorithm to successfully estimate users' data samples with arbitrarily small error probability. Combined with the results of the previous section, this implies that asymptotically (as $n \to \infty$), privacy can be achieved *if and only if* at least one of the two techniques (obfuscation or anonymization) are used above their thresholds. This statement needs a clarification as follows: Looking at the results of [73], we notice that anonymization alone can provide perfect privacy if $m(n)$ is below its threshold. On the other hand, the threshold for obfuscation requires some anonymization: In particular, the identities of the users must be permuted once to prevent the adversary from readily identifying the users.

2.4.1 Two-State i.i.d. Model

Again, we start with the i.i.d. two-state model. The data sample of user u at any time is a Bernoulli random variable with parameter p_u.

As before, we assume that p_u's are drawn independently from some continuous density function, $f_P(p_u)$, on the $(0,1)$ interval. Specifically, there are $\delta_1, \delta_2 > 0$ such that:

$$\begin{cases} \delta_1 < f_P(p_u) < \delta_2, & p_u \in (0,1). \\ f_P(p_u) = 0, & p_u \notin (0,1). \end{cases}$$

Theorem 3. For the above two-state mode, if $\mathbf{Z}$ is the obfuscated version of $\mathbf{X}$, and $\mathbf{Y}$ is the anonymized version of $\mathbf{Z}$ as defined, and

- $m \triangleq \Omega\left(cn^{2+\alpha}\right)$ for any $c > 0$ and $\alpha > 0$;
- $R_u \sim \text{Uniform}[0, a_n]$, where $a_n \triangleq O\left(c'n^{-(1+\beta)}\right)$ for any $c' > 0$ and $\beta > \frac{\alpha}{4}$;

then, user 1 no privacy at time k.

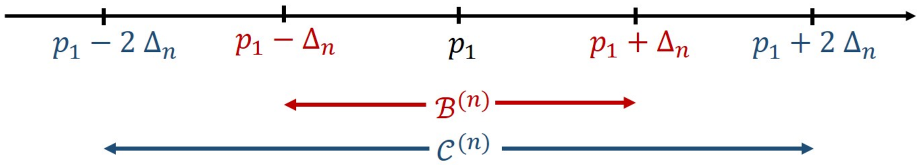


Figure 2.8: p_1, sets $\mathcal{B}^{(n)}$ and $C^{(n)}$ for case $r = 2$.

Since this is a converse result, we give an explicit detector at the adversary and show that it can be used by the adversary to recover the true data of user 1.

Proof. The adversary first inverts the anonymization mapping Π to obtain $Z_1(k)$, and then estimates the value of $X_1(k)$ from that. To invert the anonymization, the adversary calculates the empirical probability that each string is in state 1 and then assigns the string with the empirical probability closest to p_1 to user 1.

Formally, for $u = 1, 2, \cdots, n$, the adversary computes $\overline{Y_u}$, the empirical probability of user u being in state 1, as follows:

$$\overline{Y_u} = \frac{Y_u(1) + Y_u(2) + \cdots + Y_u(m)}{m},$$

thus,

$$\overline{Y_{\Pi(u)}} = \frac{Z_u(1) + Z_u(2) + \cdots + Z_u(m)}{m}.$$

As shown in Figure 2.8, define

$$\mathcal{B}^{(n)} \triangleq \left\{x \in (0,1); p_1 - \Delta_n \le x \le p_1 + \Delta_n\right\},$$

where $\Delta_n = \frac{1}{n^{1+\frac{\alpha}{4}}}$ and α is defined in the statement of Theorem 3. We claim that for $m \triangleq cn^{2+\alpha}$, $a_n \triangleq c'n^{-(1+\beta)}$, and as $n \to infty$,

1. $\mathbb{P}\left(\overline{Y_{\Pi(1)}} \in \mathcal{B}^{(n)}\right) \to 1.$

2. $\mathbb{P}\left(\bigcup\limits_{u=2}^{n}\left(\overline{Y_{\Pi(u)}} \in \mathcal{B}^{(n)}\right)\right) \to 0.$

As a result, the adversary can identify $\Pi(1)$ by examining $\overline{Y_u}$'s and assigning the one in $\mathcal{B}^{(n)}$ to user 1. Note that $\overline{Y_{\Pi(u)}} \in \mathcal{B}^{(n)}$ is a set (event) in the underlying probability space and can be written as $\left\{\omega \in \Omega : \overline{Y_{\Pi(u)}}(\omega) \in \mathcal{B}^{(n)}\right\}$.

First, we show that as n goes to infinity,

$$\mathbb{P}\left(\overline{Y_{\Pi(1)}} \in \mathcal{B}^{(n)}\right) \to 1.$$

We can write

$$\begin{aligned}
\mathbb{P}\left(\overline{Y_{\Pi(1)}} \in \mathcal{B}^{(n)}\right) &= \mathbb{P}\left(\frac{\sum\limits_{k=1}^{m} Z_1(k)}{m} \in \mathcal{B}^{(n)}\right) \\
&= \mathbb{P}\left(p_1 - \Delta_n \leq \frac{\sum\limits_{k=1}^{m} Z_1(k)}{m} \leq p_1 + \Delta_n\right) \\
&= \mathbb{P}\left(mp_1 - m\Delta_n - mQ_1 \leq \sum_{k=1}^{m} Z_1(k) - mQ_1 \leq mp_1 + m\Delta_n - mQ_1\right).
\end{aligned}$$

Note that for any $u \in \{1, 2, \cdots, n\}$, we have

$$Q_u \big| P_u = p_u \sim \text{Uniform}\left(p_u, p_u + (1 - 2p_u)a_n\right),$$

and as a result,

$$\begin{aligned}
|p_u - Q_u| &\leq |1 - 2p_u| R_u \\
&\leq R_u \leq a_n,
\end{aligned}$$

so, we can conclude

$$\mathbb{P}\left(\overline{Y_{\Pi(1)}} \in \mathcal{B}^{(n)}\right) = \mathbb{P}\left(mp_1 - m\Delta_n - mQ_1 \leq \sum_{k=1}^{m} Z_1(k) - mQ_1 \leq mp_1 + m\Delta_n - mQ_1\right)$$

$$
\begin{aligned}
&\geq \mathbb{P}\left(-m\Delta_n + ma_n \leq \sum_{k=1}^{m} Z_1(k) - mQ_1 \leq -ma_n + m\Delta_n\right) \\
&= \mathbb{P}\left(\left|\sum_{k=1}^{m} Z_1(k) - mQ_1\right| \leq m(\Delta_n - a_n)\right).
\end{aligned}
$$

From the Chernoff bound, for any $c, c', \alpha > 0$ and $\beta > \frac{\alpha}{4}$,

$$
\begin{aligned}
\mathbb{P}\left(\left|\sum_{k=1}^{m} Z_1(k) - mQ_1\right| \leq m(\Delta_n - a_n)\right) &\geq 1 - 2e^{-\frac{m(\Delta_n - a_n)^2}{3Q_1}} \\
&\geq 1 - 2e^{-\left(\frac{1}{3Q_1}\right)\left(cn^{2+\alpha}\right)\left(\frac{1}{n^{1+\frac{\alpha}{4}}} - \frac{c'}{n^{1+\beta}}\right)^2} \\
&\geq 1 - 2e^{-\frac{1}{3}\left(cn^{2+\alpha}\right)\left(\frac{1}{n^{1+\frac{\alpha}{4}}} - \frac{c'}{n^{1+\beta}}\right)^2} \longrightarrow 1.
\end{aligned}
$$

As a result, as n becomes large,

$$
\mathbb{P}\left(\overline{Y_{\Pi(1)}} \in \mathcal{B}^{(n)}\right) \longrightarrow 1.
$$

Now, we need to show that as n goes to infinity,

$$
\mathbb{P}\left(\bigcup_{u=2}^{n}\left(\overline{Y_{\Pi(u)}} \in \mathcal{B}^{(n)}\right)\right) \longrightarrow 0.
$$

First, we define

$$
\mathcal{C}^{(n)} = \left\{x \in (0,1); p_1 - 2\Delta_n \leq x \leq p_1 + 2\Delta_n\right\},
$$

and claim as n goes to infinity,

$$
\mathbb{P}\left(\bigcup_{u=2}^{n}\left(P_u \in \mathcal{C}^{(n)}\right)\right) \longrightarrow 0.
$$

Note

$$
4\Delta_n\delta_1 < \mathbb{P}\left(P_u \in \mathcal{C}^{(n)}\right) < 4\Delta_n\delta_2,
$$

and according to the union bound, as $n \to \infty$,

$$\begin{aligned}\mathbb{P}\left(\bigcup_{u=2}^{n}\left(P_u \in C^{(n)}\right)\right) &\le \sum_{u=2}^{n}\mathbb{P}\left(P_u \in C^{(n)}\right)\\ &\le 4n\Delta_n\delta_2\\ &= 4n\frac{1}{n^{1+\frac{\alpha}{4}}}\delta_2\\ &= 4n^{-\frac{\alpha}{4}}\delta_2 \to 0.\end{aligned}$$

As a result, we can conclude that all p_u's are outside of $C^{(n)}$ for $u \in \{2, 3, \cdots, n\}$ with high probability.

Now, we claim that given all p_u's are outside of $C^{(n)}$, $\mathbb{P}\left(\overline{Y_{\Pi(u)}} \in \mathcal{B}^{(n)}\right)$ is small. Remember that for any $u \in \{1, 2, \cdots, n\}$, we have

$$|p_u - Q_u| \le a_n.$$

Now, noting the definitions of sets $\mathcal{B}^{(n)}$ and $C^{(n)}$, we can write for $u \in \{2, 3, \cdots, n\}$,

$$\begin{aligned}\mathbb{P}\left(\overline{Y_{\Pi(u)}} \in \mathcal{B}^{(n)}\right) &\le \mathbb{P}\left(\left|\overline{Y_{\Pi(u)}} - Q_u\right| \ge (\Delta_n - a_n)\right)\\ &= \mathbb{P}\left(\left|\sum_{k=1}^{m} Z_u(k) - mQ_u\right| > m(\Delta_n - a_n)\right).\end{aligned}$$

According to the Chernoff bound, for any $c, c', \alpha > 0$ and $\beta > \frac{\alpha}{4}$,

$$\begin{aligned}\mathbb{P}\left(\left|\sum_{k=1}^{m} Z_u(k) - mQ_u\right| > m(\Delta_n - a_n)\right) &\le 2e^{-\frac{m(\Delta_n - a_n)^2}{3Q_1}}\\ &\le 2e^{-\left(\frac{1}{3Q_1}\right)\left(cn^{2+\alpha}\right)\left(\frac{1}{n^{1+\frac{\alpha}{4}}} - \frac{c'}{n^{1+\beta}}\right)^2}\\ &\le 2e^{-\frac{1}{3}\left(cn^{2+\alpha}\right)\left(\frac{1}{n^{1+\frac{\alpha}{4}}} - \frac{c'}{n^{1+\beta}}\right)^2}.\end{aligned}$$

Now, by using a union bound, for any $\beta > \frac{\alpha}{4}$, we have

$$\begin{aligned}
\mathbb{P}\left(\bigcup_{u=2}^{n}\left(\overline{Y_{\Pi(u)}} \in \mathcal{B}^{(n)}\right)\right) &\leq \sum_{u=2}^{n} \mathbb{P}\left(\overline{Y_{\Pi(u)}} \in \mathcal{B}^{(n)}\right) \\
&\leq n\left(2e^{-\frac{1}{3}\left(cn^{2+\alpha}\right)\left(\frac{1}{n^{1+\frac{\alpha}{4}}}-\frac{c'}{n^{1+\beta}}\right)^{2}}\right),
\end{aligned}$$

and thus, as n goes to infinity,

$$\mathbb{P}\left(\bigcup_{u=2}^{n}\left(\overline{Y_{\Pi(u)}} \in \mathcal{B}^{(n)}\right)\right) \to 0.$$

So, the adversary can successfully recover $Z_1(k)$. Since $Z_1(k) = X_1(k)$ with probability $1 - R_1 = 1 - o(1)$, the adversary can recover $X_1(k)$ with vanishing error probability as $n \to \infty$. □

2.4.2 r-State i.i.d. Model

Now, assume users' data samples can have r possibilities $(0, 1, \cdots, r-1)$, and $p_u(i)$ shows the probability of user u having data sample i. We define the vector $\mathbf{p}_u$ and the matrix $\mathbf{p}$ as

$$\mathbf{p}_u = \begin{bmatrix} p_u(1) \\ \\ p_u(2) \\ \\ \vdots \\ \\ p_u(r-1) \end{bmatrix}, \quad \mathbf{p} = \left[\mathbf{p}_1, \mathbf{p}_2, \cdots, \mathbf{p}_n\right].$$

We also assume $\mathbf{p}_u$'s are drawn independently from some continuous density function, $f_P(\mathbf{p}_u)$, which has support on a subset of the $(0,1)^{r-1}$ hypercube. In particular, define the range of distribution as

$$\mathcal{R}_{\mathbf{p}} = \left\{(x_1, x_2, \cdots, x_{r-1}) \in (0,1)^{r-1} : x_i > 0, x_1 + x_2 + \cdots + x_{r-1} < 1, \;\; i = 1, 2, \cdots, r-1\right\}$$

Then, we assume there are $\delta_1, \delta_2 > 0$ such that:

$$\begin{cases} \delta_1 < f_{\mathbf{P}}(\mathbf{p}_u) < \delta_2, & \mathbf{p}_u \in \mathcal{R}_{\mathbf{p}}. \\ f_{\mathbf{P}}(\mathbf{p}_u) = 0, & \mathbf{p}_u \notin \mathcal{R}_{\mathbf{p}}. \end{cases}$$

Theorem 4. For the above r-state mode, if $\mathbf{Z}$ is the obfuscated version of $\mathbf{X}$, and $\mathbf{Y}$ is the anonymized version of $\mathbf{Z}$ as defined, and

- $m \triangleq \Omega\left(cn^{\frac{2}{r-1}+\alpha}\right)$ for any $c > 0$ and $0 < \alpha < 1$;
- $R_u \sim \text{Uniform}[0, a_n]$, where $a_n \triangleq O\left(c'n^{-\left(\frac{1}{r-1}+\beta\right)}\right)$ for any $c' > 0$ and $\beta > \frac{\alpha}{4}$;

then, user 1 no privacy at time k.

The proof of Theorem 4 is similar to the proof of Theorem 3, so we just provide the general idea. We similarly define the empirical probability that the user with pseudonym u has data sample i $\left(\overline{Y_u}(i)\right)$ as follows:

$$\overline{Y_u}(i) = \frac{|\{k \in \{1, 2, \cdots, m\} : Y_u(k) = i\}|}{m},$$

thus,

$$\overline{Y_{\Pi(u)}}(i) = \frac{|\{k \in \{1, 2, \cdots, m\} : Y_u(k) = i\}|}{m}.$$

The difference is that now for each $u \in \{1, 2, \cdots, n\}$, $\overline{\mathbf{Y}_u}$ is a vector of size $r-1$. In other words,

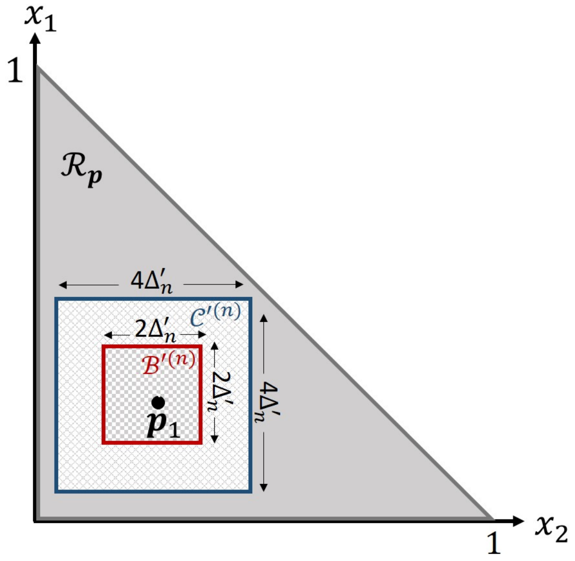


Figure 2.9: $\mathbf{p}_1$, sets $\mathcal{B}'^{(n)}$ and $\mathcal{C}'^{(n)}$ in $\mathcal{R}_\mathbf{p}$ for case $r = 3$.

$$\overline{\mathbf{Y}_u} = \begin{bmatrix} \overline{Y_u}(1) \\ \\ \overline{Y_u}(2) \\ \\ \vdots \\ \\ \overline{Y_u}(r-1) \end{bmatrix}.$$

Define sets $\mathcal{B}'^{(n)}$ and $\mathcal{C}'^{(n)}$ as

$$\mathcal{B}'^{(n)} \triangleq \left\{(x_1, x_2, \cdots, x_{r-1}) \in \mathcal{R}_\mathbf{p} : p_1(i) - \Delta'_n \leq x_i \leq p_1(i) + \Delta'_n,\ i = 1, 2, \cdots, r-1\right\},$$

$$\mathcal{C}'^{(n)} \triangleq \left\{(x_1, x_2, \cdots, x_{r-1}) \in \mathcal{R}_\mathbf{p} : p_1(i) - 2\Delta'_n \leq x_i \leq p_1(i) + 2\Delta'_n,\ i = 1, 2, \cdots, r-1\right\},$$

where $\Delta'_n = \frac{1}{n^{\frac{1}{r-1}+\frac{\alpha}{4}}}$. Figure 2.9 shows $\mathbf{p}_1$ and sets $\mathcal{B}'^{(n)}$ and $\mathcal{C}'^{(n)}$ for the case $r = 3$.

We claim for $m \triangleq cn^{\frac{2}{r-1}+\alpha}$, $a_n \triangleq c'n^{-\left(\frac{1}{r-1}+\beta\right)}$, as $n \to \infty$,

1. $\mathbb{P}\left(\overline{\mathbf{Y}_{\Pi(1)}} \in \mathcal{B}'^{(n)}\right) \to 1.$

2. $\mathbb{P}\left(\bigcup_{u=2}^{n}\left(\overline{\mathbf{Y}_{\Pi(u)}} \in \mathcal{B}'^{(n)}\right)\right) \to 0.$

The proof follows that for the two-state case. Thus, the adversary can de-anonymize the data and then recover $X_1(k)$ with vanishing error probability in the r-state model.

2.4.3 r-State Markov Chain Model

So far, we have assumed users' data samples can have r possibilities $(0, 1, \cdots, r-1)$ and users' pattern are i.i.d. . Here we model users' pattern using Markov chains to capture the dependency of the users' pattern over time. Again, we assume there are r possibilities (the number of states in the Markov chains). Let E be the set of edges. More specifically, $(i, j) \in E$ if there exists an edge from i to j with probability $p(i, j) > 0$. What distinguishes different users is their transition probabilities $p_u(i, j)$ (the probability that user u jumps from state i to state j). The adversary knows the transition probabilities of all users. The model for obfuscation and anonymization is exactly the same as before.

We show that the adversary will be able to estimate the data samples of the users with low error probability if $m(n)$ and a_n are in the appropriate range. The key idea is that the adversary can focus on a subset of the transition probabilities that are sufficient for recovering the entire transition probability matrix. By estimating those transition probabilities from the observed data and matching with the known transition probabilities of the users, the adversary will be able to first de-anonymize the data, and then estimate the actual samples of users' data. In particular, note that for each state i, we must have

$$\sum_{j=1}^{r} p_u(i, j) = 1, \quad \text{for each } u \in \{1, 2, \cdots, n\},$$

so, the Markov chain of user u is completely determined by a subset of size $d = |E| - r$ of transition probabilities. We define the vector $\mathbf{p}_u$ and the matrix $\mathbf{p}$ as

$$\mathbf{p}_u = \begin{bmatrix} p_u(1) \\ p_u(2) \\ \vdots \\ p_u(|E|-r) \end{bmatrix}, \quad \mathbf{p} = \left[\mathbf{p}_1, \mathbf{p}_2, \cdots, \mathbf{p}_n\right].$$

We also consider $\mathbf{p}_u$'s are drawn independently from some continuous density function, $f_P(\mathbf{p}_u)$, which has support on a subset of the $(0,1)^{|E|-r}$ hypercube. Let $\mathcal{R}_{\mathbf{p}} \subset \mathbb{R}^d$ be the range of acceptable values for $\mathbf{p}_u$, so we have

$$\mathcal{R}_{\mathbf{P}} = \left\{(x_1, x_2 \cdots, x_d) \in (0,1)^d : x_i > 0, x_1 + x_2 + \cdots + x_d < 1, \ i = 1, 2, \cdots, d\right\}.$$

As before, we assume there are $\delta_1, \delta_2 > 0$, such that:

$$\begin{cases} \delta_1 < f_{\mathbf{P}}(\mathbf{p}_u) < \delta_2, & \mathbf{p}_u \in \mathcal{R}_{\mathbf{p}}. \\ f_{\mathbf{P}}(\mathbf{p}_u) = 0, & \mathbf{p}_u \notin \mathcal{R}_{\mathbf{p}}. \end{cases}$$

Using the above observations, we can establish the following theorem.

Theorem 5. For an irreducible, aperiodic Markov chain with r states and $|E|$ edges as defined above, if $\mathbf{Z}$ is the obfuscated version of $\mathbf{X}$, and $\mathbf{Y}$ is the anonymized version of $\mathbf{Z}$, and

- $m \triangleq \Omega\left(cn^{\frac{2}{|E|-r}+\alpha}\right)$ for any $c > 0$ and $\alpha > 0$;
- $R_u \sim \text{Uniform}[0, a_n]$, where $a_n \triangleq O\left(c' n^{-\left(\frac{1}{|E|-r}+\beta\right)}\right)$ for any $c' > 0$ and $\beta > \frac{\alpha}{4}$;

then, user 1 no privacy at time k.

The proof has a lot of similarity to the i.i.d. case, so we provide a sketch, mainly focusing on the differences. We argue as follows. If the total number of observations per user is $m = m(n)$, then define $M_i(u)$ to be the total number of visits by user u to state i, for $i = 0, 1, \cdots, r-1$. Since the Markov chain is irreducible and aperiodic, and $m(n) \to \infty$, all $\frac{M_i(u)}{m(n)}$ converge to their stationary values. Now conditioned on $M_i(u) = m_i(u)$, the transitions from state i to state l for user u follow a multinomial distribution with probabilities $p_u(i, l)$.

Given the above, the setting is now very similar to the i.i.d. case. Each user is uniquely characterized by a vector $\mathbf{p}_u$ of size $|E| - r$. We define sets $\mathcal{B}^{''(n)}$ and $C^{''(n)}$ as

$$\mathcal{B}^{''(n)} \triangleq \{(x_1, x_2, \cdots, x_d) \in \mathcal{R}_{\mathbf{p}} : p_1(i) - \Delta''_n \leq x_i \leq p_1(i) + \Delta''_n, i = 1, 2, \cdots, d\},$$

$$C^{''(n)} \triangleq \{(x_1, x_2, \cdots, x_d) \in \mathcal{R}_{\mathbf{p}} : p_1(i) - 2\Delta''_n < x_i < p_1(i) + 2\Delta''_n, i = 1, 2, \cdots, d\},$$

where $\Delta''_n = \frac{1}{n^{\frac{1}{|E|-r} + \frac{\alpha}{4}}}$, and $d = |E| - r$. Then, we can show that for the stated values of $m(n)$ and a_n, as n becomes large:

1. $\mathbb{P}\left(\overline{\mathbf{Y}_{\Pi(1)}} \in \mathcal{B}^{''(n)}\right) \to 1,$
2. $\mathbb{P}\left(\bigcup\limits_{u=2}^{n} \left(\overline{\mathbf{Y}_{\Pi(u)}} \in B''^{(n)}\right)\right) \to 0,$

which means that the adversary can estimate the data of user 1 with vanishing error probability. The proof is very similar to the proof of the i.i.d. case; however, there are two differences that need to be addressed:

First, the probability of observing an erroneous observation is not exactly given by R_u. In fact, a transition is distorted if at least one of its nodes is distorted. So, if the actual transition is from state i to state l, then the probability of an erroneous observation is equal to

$$R'_u = R_u + R_u - R_u R_u = R_u(2 - R_u).$$

Nevertheless, here the order only matters, and the above expression is still in the order of $a_n = O\left(n^{-\left(\frac{1}{|E|-r}+\beta\right)}\right)$.

The second difference is more subtle. As opposed to the i.i.d. case, the error probabilities are not completely independent. In particular, if $X_u(k)$ is reported in error, then both the transition to that state and from that state are reported in error. This means that there is a dependency between errors of adjacent transitions. We can address this issue in the following way: The adversary makes their decision only based on a subset of the observations. More specifically, the adversary looks at only odd-numbered transitions: First, third, fifth, etc., and ignores the even-numbered transitions. In this way, the number of observations is effectively reduced from m to $\frac{m}{2}$ which again does not impact the order of the result (recall that the Markov chain is aperiodic). However, the adversary now has access to observations with independent errors.

2.5 Perfect Privacy Analysis: $r-$ State Markov Chain Model

So far, we have provided both achievability and converse results for the i.i.d. case. However, we have only provided the converse results for the Markov chain case. Here, we investigate achievability for Markov chain models. It turns out that for this case, the assumed obfuscation technique is not sufficient to achieve a reasonable level of privacy. Loosely speaking, we can state that if the adversary can make enough observations, then he can break the anonymity. The culprit is the fact that the sequence observed by the adversary is no longer modeled by a Markov chain; rather, it can be modeled by a hidden Markov chain. This allows the adversary to successfully estimate the obfuscation random variable R_u as well as the $p_u(i,l)$ values for each sequence, and hence successfully de-anonymize the sequences.

More specifically, as we will see below, there is a fundamental difference between the i.i.d. case and the Markov chain case. In the i.i.d. case, if the noise level is beyond a relatively small threshold, the adversary will be unable to de-anonymize the data and unable to recover the actual values of the data sets for users, *regardless of the (large) size of* $m = m(n)$. On the other hand, in the Markov chain case, if $m = m(n)$ is large enough, then the adversary can easily de-anonymize the data. To better illustrate this, let us consider a simple example.

Example 1. Consider the scenario where there are only two states and the users' data samples change between the two states according to the Markov chain shown in Figure 2.10. What distinguishes the users is their different values of p_u. Now, suppose we use the same obfuscation method as before. That is, to create a noisy version of the sequences of data samples, for each user u, we generate the random variable R_u that is the probability that the data sample of the user is changed to a different data sample by obfuscation. Specifically,

$$Z_u(k) = \begin{cases} X_u(k), & \text{with probability } 1 - R_u. \\ 1 - X_u(k), & \text{with probability } R_u. \end{cases}$$

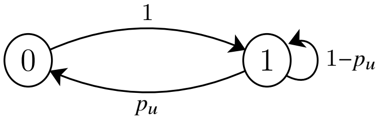


Figure 2.10: A state transition diagram.

To analyze this problem, we can construct the underlying Markov chain as follows. Each state in this Markov chain is identified by two values: the real state of the user, and the observed value by the adversary. In particular, we can write

$$(\text{Real value}, \text{Observed value}) \in \{(0,0), (0,1), (1,0), (1,1)\}.$$

Figure 2.11 shows the state transition diagram of this new Markov chain.

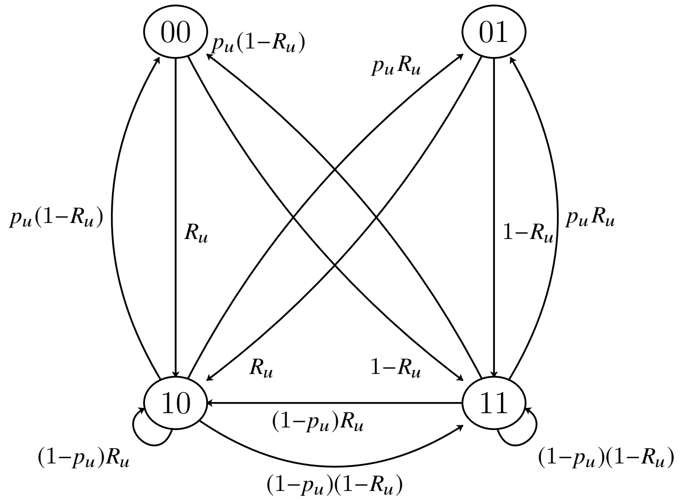


Figure 2.11: The state transition diagram of the new Markov chain.

We know

$$\pi_{00} = \pi_0(1 - R_u) = \frac{p_u}{1 + p_u}(1 - R_u).$$

$$\pi_{01} = \pi_0 R_u = \frac{p_u}{1 + p_u} R_u.$$

$$\pi_{10} = \pi_1 R_u = \frac{1}{1 + p_u} R_u.$$

$$\pi_{11} = \pi_1(1 - R_u) = \frac{1}{1 + p_u}(1 - R_u).$$

The observed process by the adversary is not a Markov chain; nevertheless, we can define limiting probabilities. In particular, let θ_0 be the limiting probability of observing a zero. That is, we have

$$\frac{M_0}{m} \xrightarrow{d} \theta_0, \quad \text{as } n \longrightarrow \infty,$$

where m is the total number of observations by the adversary, and M_0 is the number of 0's observed. Then,

$$\theta_0 = \pi_{00} + \pi_{10} = \frac{(1 - R_u)p_u + R_u}{1 + p_u}.$$

Also, let θ_1 be the limiting probability of observing a one, so

$$\theta_1 = \pi_{01} + \pi_{11} = \frac{p_u R_u + (1 - R_u)}{1 + p_u} = 1 - \theta_0.$$

Now the adversary's estimate of θ_0 is given by:

$$\widetilde{\theta_0} = \frac{(1 - R_u)p_u + R_u}{1 + p_u}. \tag{2.1}$$

Note that if the number of observations by the adversary can be arbitrarily large, the adversary can obtain an arbitrarily accurate estimate of θ_0. The adversary can obtain another equation easily, as follows. Let θ_{01} be the limiting value of the portion of transitions from state 0 to 1 in the chain observed by the adversary. We can write

$$\begin{aligned}\theta_{01} &= P\left\{(00 \to 01), (00 \to 11), (10 \to 01), (10 \to 11)\right\}\\ &= \pi_{00}(1 - R_u) + \pi_{10} p_u R_u + \pi_{10}(1 - p_u)(1 - R_u).\end{aligned}$$

As a result,

$$\widetilde{\theta_{01}} = \frac{p_u(1 - R_u)^2 + R_u\left(p_u R_u (1 - R_u)(1 - p_u)\right)}{1 + p_u}. \tag{2.2}$$

Again, if the number of observations can be arbitrarily large, the adversary can obtain an arbitrarily accurate estimate of θ_{01}. By solving (2.1) and (2.2), the adversary can successfully recover R and p; thus, they can successfully determine the users' data values.

2.6 Discussion

2.6.1 Markov Chain Model

As opposed to the i.i.d. case, we see from Section 2.5 that if we do not limit $m = m(n)$, the assumed obfuscation method will not be sufficient to achieve perfect privacy. There are a few natural questions here. First, for a given noise level, what would be the maximum $m(n)$ that could guarantee perfect privacy in this model? The more interesting question is, how can we possibly modify the obfuscation technique to make it more suitable for the Markov chain model? A natural solution seems to be re-generating the obfuscation random variables R_u periodically. This will keep the adversary from easily estimating them by observing a long sequence of data at a small increase in complexity. In fact, this will make the obfuscation much more *robust* to modeling uncertainties and errors. It is worth noting, however, that this change would not affect the other results in this chapter. That is, even if the obfuscation random variables are re-generated frequently, it is relatively easy to check that all the previous theorems in this chapter remain valid. However, the increase in robustness to modeling errors will definitely be a significant advantage. Thus, the question is how often should the random variable R_u be re-generated to strike a good balance between complexity and privacy? These are all interesting questions for future research.

2.6.2 Obfuscating the Samples of Users' Data Using Continuous Noise

Here we argue that for the setting of this chapter, continuous noise such as that drawn from a Gaussian distribution is not a good option to obfuscate the sample of users' data drawn from a finite alphabet when we want to achieve perfect privacy. For a better understanding, let us consider a simple example.

Example 2. Consider the scenario where the users' datasets are governed by an i.i.d. model and the number of possible values for each sample of the users' data (r) is equal to 2 (two-state model). Note that the data sequence for user u is a Bernoulli random variable with parameter p_u.

Assume that the actual sample of the data of user u at time k ($X_u(k)$) is obfuscated using noise drawn from a Gaussian distribution ($S_u(k)$), and $Z_u(k)$ is the obfuscated version of $X_u(k)$. That is, we can write

$$Z_u(k) = X_u(k) + S_u(k);$$

where $S_u(k) \sim N\left(\mu(R_u), \sigma^2(R_u)\right)$, is independent of $X_u(k)$, and R_u is the noise parameter which is chosen from some distribution. Here, $\mu(R_u)$ and $\sigma^2(R_u)$ are some known functions of R_u. We also apply anonymization to $Z_u(k)$, and, as before, $Y_u(k)$ is the reported sample of the data of user u at time k after applying anonymization. Per Section 2.2, anonymization is modeled by a random permutation $\Pi(u)$ on the set of n users.

Now, the question is as follows: Is it possible to achieve perfect privacy independent of the number of adversary's observation (m) while using this continuous noise ($S_u(k)$) to obfuscate the sample of users' data?

Note that

$$E[Z_u(k)] = p_u + \mu(R_u), \tag{2.3}$$

and

$$Var\left(Z_u(k)\right) = p_u(1 - p_u) + \sigma^2(R_u). \tag{2.4}$$

In this case, when the adversary's number of observations is arbitrarily large, the adversary can obtain good estimates of $E[Z_u(k)]$ and $Var\left(Z_u(k)\right)$ for each user with an arbitrarily small error probability. Then, by using (2.3) and (2.4), the adversary can recover p_u and R_u. As a result, the adversary can de-anonymize the data and then recover $X_u(k)$. The conclusion here is that a continuous noise distribution can potentially give information to the adversary when used for obfuscation of finite alphabet data. A method to mitigate this issue is to regenerate the random variables R_u frequently (similar to our previous discussion for Markov chains). Understanding the optimal frequency of such a regeneration and detailed analysis in this case is an interesting future research direction.

2.7 Summary of the Results

Given n, the total number of the users in a network, their degree of privacy depends on two parameters: (1) The number of observations $m = m(n)$ by the adversary per user for a fixed anonymization mapping (i.e., the number of observations before the pseudonyms are changed); and (2) the value of the noise added by the obfuscation technique. Intuitively, smaller $m(n)$ and larger a_n result in stronger privacy, at the expense of lower utility for the users. When the users' datasets are governed by an i.i.d. process, we showed that the $m(n)-a_n$ plane can be divided into two areas. In the first area, all users have perfect privacy (as defined in Section 2.2), and, in the second area, users have no privacy. Figure 2.12 shows the limits of privacy in the entire $m(n) - a_n$ plane. As the figure shows, number of adversary's observations per user (m) is significantly smaller than $n^{\frac{2}{r-1}}$ or the amount of noise level (a_n) is significantly larger than $n^{-\frac{1}{r-1}}$, users have perfect privacy and if the levels of both anonymization adn obfuscation them are significantly low, users have no privacy.

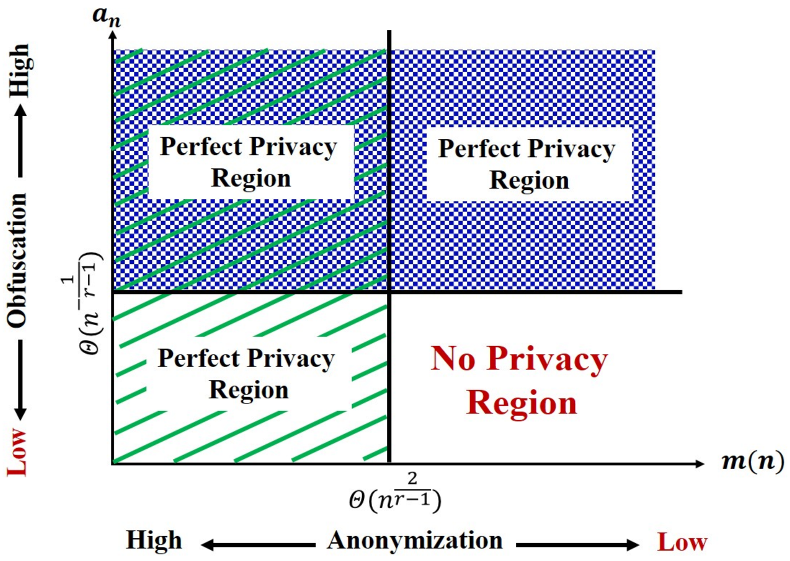


Figure 2.12: Limits of privacy in the entire $m(n) - a_n$ plane. Note that $m(n)$ is the number of the adversary's observations per user (degree of anonymization), and a_n is the amount of noise level (degree of obfuscation).

For the case where the users' datasets are governed by irreducible and aperiodic Markov chains with r states and $|E|$ edges, we show that users will have no privacy if $m = cn^{\frac{2}{|E|-r}+\alpha}$ and $a_n = c'n^{-\left(\frac{1}{|E|-r}+\beta\right)}$, for any constants $c > 0$, $c' > 0$, $\alpha > 0$, and $\beta > \frac{\alpha}{4}$. We also provide some insights for the opposite direction (under which conditions users have perfect privacy) for the case of Markov chains.

2.8 Appendix

2.8.1 Lemma 6 and its Proof

Here we state that we can condition on high-probability events.

Lemma 6. Let $p \in (0,1)$, and $X \sim Bernoulli(p)$ be defined on a probability space $(\Omega, \mathcal{F}, P)$. Consider $B_1, B_2, \cdots$ be a sequence of events defined on the same probability space such that $\mathbb{P}(B_n) \to 1$ as n goes to infinity. Also, let $\mathbf{Y}$ be a random vector (matrix) in the same probability space, then:

$$\mathbb{I}(X;\mathbf{Y}) \to 0 \text{ iff } \mathbb{I}(X;\mathbf{Y}|B_n) \to 0.$$

Proof. First, we prove that as n becomes large,

$$H(X|B_n) - H(X) \to 0. \tag{2.5}$$

Note that as n goes to infinity,

$$\begin{aligned}\mathbb{P}(X=1) &= \mathbb{P}\left(X=1\middle|B_n\right)\mathbb{P}(B_n) + \mathbb{P}\left(X=1\middle|\overline{B_n}\right)\mathbb{P}\left(\overline{B_n}\right)\\ &= \mathbb{P}\left(X=1\middle|B_n\right),\end{aligned}$$

thus, $\left(X\middle|B_n\right) \xrightarrow{d} X$, and as n goes to infinity,

$$H(X|B_n) - H(X) \to 0.$$

Similarly, as n becomes large,

$$\mathbb{P}\left(X = 1\middle|\mathbf{Y} = \mathbf{y}\right) \to \mathbb{P}\left(X = 1\middle|\mathbf{Y} = \mathbf{y}, B_n\right),$$

and

$$H\left(X|\mathbf{Y} = \mathbf{y}, B_n\right) - H\left(X|\mathbf{Y} = \mathbf{y}\right) \to 0. \tag{2.6}$$

Remembering that

$$\mathbb{I}(X;\mathbf{Y}) = H(X) - H(X|\mathbf{Y}), \tag{2.7}$$

and using (2.5), (2.6), and (2.7), we can conclude that as n goes to infinity,

$$\mathbb{I}\left(X;\mathbf{Y}|B_n\right) - \mathbb{I}\left(X,\mathbf{Y}\right) \to 0.$$

As a result, as $n \to \infty$,

$$\mathbb{I}\left(X;\mathbf{Y}\right) \to 0 \Longleftrightarrow \mathbb{I}\left(X;\mathbf{Y}|B_n\right) \to 0.$$

□

2.8.2 Proof of Lemma 1

Here we provide a formal proof for Lemma 1 which we restate as follows. Let N be a positive integer, and let $a_1, a_2, \cdots, a_N$ and $b_1, b_2, \cdots, b_N$ be real numbers such that $a_u \leq b_u$ for all u. Assume that $X_1, X_2, \cdots, X_N$ are N independent random variables such that

$$X_u \sim Uniform[a_u, b_u].$$

Let also $\gamma_1, \gamma_2, \cdots, \gamma_N$ be real numbers such that

$$\gamma_j \in \bigcap_{u=1}^{N} [a_u, b_u] \text{ for all } j \in \{1, 2, \cdots, N\}.$$

Suppose that we know the event E has occurred, meaning that the observed values of X_u's is equal to the set of γ_j's (but with unknown ordering), i.e.,

$$E \equiv \{X_1, X_2, \cdots, X_N\} = \{\gamma_1, \gamma_2, \cdots, \gamma_N\},$$

then

$$\mathbb{P}\left(X_1 = \gamma_j | E\right) = \frac{1}{N}.$$

Proof. Define sets $\mathfrak{P}$ and $\mathfrak{P}_j$ as follows:

$$\mathfrak{P} = \text{The set of all permutations } \Pi \text{ on } \{1, 2, \cdots, N\}.$$

$$\mathfrak{P}_j = \text{The set of all permutations } \Pi \text{ on } \{1, 2, \cdots, N\} \text{ such that } \Pi(1) = j.$$

We have $|\mathfrak{P}| = N!$ and $|\mathfrak{P}| = (N-1)!$. Then

$$\begin{aligned}
\mathbb{P}(X_1 = \alpha_j | E) &= \frac{\sum_{\pi \in \mathfrak{P}_j} f_{X_1, X_2, \cdots, X_N}\left(\gamma_{\pi(1)}, \gamma_{\pi(2)}, \cdots, \gamma_{\pi(N)}\right)}{\sum_{\pi \in \mathfrak{P}} f_{X_1, X_2, \cdots, X_N}\left(\gamma_{\pi(1)}, \gamma_{\pi(2)}, \cdots, \gamma_{\pi(N)}\right)} \\
&= \frac{(N-1)! \prod\limits_{u=1}^{N} \frac{1}{b_u - a_u}}{N! \prod\limits_{u=1}^{N} \frac{1}{b_u - a_u}} \\
&= \frac{1}{N}.
\end{aligned}$$

□

2.8.3 Proof of Lemma 4

Here, we provide a formal proof for Lemma 4 which we restate as follows. The following lemma confirms that the number of elements in $J^{(n)}$ goes to infinity as n becomes large.

If $N^{(n)} \triangleq |J^{(n)}|$, then $N^{(n)} \to \infty$ with high probability as $n \to \infty$. More specifically, there exists $\lambda > 0$ such that

$$\mathbb{P}\left(N^{(n)} > \frac{\lambda}{2} n^{\frac{\beta}{2}}\right) \longrightarrow 1.$$

Proof. Define the events A, B as

$$A \equiv p_1 \leq P_u \leq p_1 + \epsilon_n$$

$$B \equiv p_1 + \epsilon_n \leq Q_u \leq p_1 + (1 - 2p_1)a_n.$$

Then, for $u \in \{1, 2, \dots, n\}$ and $0 \leq p_1 < \frac{1}{2}$:

$$\begin{aligned}\mathbb{P}\left(u \in J^{(n)}\right) &= \mathbb{P}\left(A \ \cap \ B\right) \\ &= \mathbb{P}\left(A\right) \mathbb{P}\left(B \middle| A\right).\end{aligned}$$

So, given $p_1 \in (0, 1)$ and the assumption $0 < \delta_1 < f_p < \delta_2$, for n large enough, we have

$$\mathbb{P}(A) = \int_{p_1}^{p_1 + \epsilon_n} f_P(p) dp,$$

so, we can conclude that

$$\epsilon_n \delta_1 < \mathbb{P}(A) < \epsilon_n \delta_2.$$

We can find a δ such that $\delta_1 < \delta < \delta_2$ and

$$\mathbb{P}(A) = \epsilon_n \delta. \tag{2.8}$$

We know

$$Q_u \Big| P_u = p_u \sim Uniform\left[p_u, p_u + (1-2p_u)a_n\right],$$

so, according to Figure 2.5, for $p_1 \leq p_u \leq p_1 + \epsilon_n$,

$$\begin{aligned}
\mathbb{P}\left(B|P_u = p_u\right) &= \frac{p_1 + (1-2p_1)a_n - p_1 - \epsilon_n}{p_u + (1-2p_u)a_n - p_u} \\
&= \frac{(1-2p_1)a_n - \epsilon_n}{(1-2p_u)a_n} \\
&\geq \frac{(1-2p_1)a_n - \epsilon_n}{(1-2p_1)a_n} \\
&= 1 - \frac{\epsilon_n}{(1-2p_1)a_n},
\end{aligned}$$

which implies

$$\mathbb{P}\left(B|A\right) \geq 1 - \frac{\epsilon_n}{(1-2p_1)a_n}. \tag{2.9}$$

Using (2.8) and (2.9), we can conclude

$$\mathbb{P}\left(u \in J^{(n)}\right) \geq \epsilon_n \delta \left(1 - \frac{\epsilon_n}{(1-2p_1)a_n}\right).$$

Then, we can say that $N^{(n)}$ has a binomial distribution with expected value of $N^{(n)}$ greater than $n\epsilon_n\delta\left(1 - \frac{\epsilon_n}{(1-2p_1)a_n}\right)$, and by substituting ϵ_n and a_n, for any $c' > 0$, we get

$$\mathbb{E}\left[N^{(n)}\right] \geq \delta\left(n^{\frac{\beta}{2}} - \frac{1}{c'(1-2p_1)}\right) \geq \lambda n^{\frac{\beta}{2}}.$$

Now by using Chernoff bound, we have

$$\mathbb{P}\left(N^{(n)} \leq (1-\theta)\mathbb{E}\left[N^{(n)}\right]\right) \leq e^{-\frac{\theta^2}{2}\mathbb{E}\left[N^{(n)}\right]},$$

so, if we assume $\theta = \frac{1}{2}$, we can conclude as $n \to \infty$,

$$\begin{aligned}
\mathbb{P}\left(N^{(n)} \leq \frac{\lambda}{2} n^{\frac{\beta}{2}}\right) &\leq \mathbb{P}\left(N^{(n)} \leq \frac{\mathbb{E}\left[N^{(n)}\right]}{2}\right) \\
&\leq e^{-\frac{\mathbb{E}[N^{(n)}]}{8}} \\
&\leq e^{-\frac{\lambda n^{\frac{\beta}{2}}}{8}} \to 0.
\end{aligned}$$

As a result, $N^{(n)} \to \infty$ with high probability as $n \to \infty$. □

2.8.4 Completion of Proof of Lemma 5

Let $p_1 \in (0,1)$, and let $N^{(n)}$ be a random variable as above, i.e., $N^{(n)} \to \infty$ as $n \to \infty$. Consider the sequence of independent random variables $Y_u \sim Bernoulli(p_u)$ for $u = 1, 2, \cdots, N^{(n)}$ such that

1. For all n and all $u \in \left\{1, 2, \cdots, N^{(n)}\right\}$, $|p_u - p_1| \leq \zeta_n$.

2. $\lim\limits_{n\to\infty} \zeta_n = 0$.

Define

$$\overline{Y} \triangleq \frac{1}{N^{(n)}} \sum_{u=1}^{N^{(n)}} Y_u,$$

then $\overline{Y} \xrightarrow{d} p_1$.

Proof. Note

$$\begin{aligned}
\mathbb{E}[\overline{Y}] &= \frac{1}{N^{(n)}} \sum_{u=1}^{N^{(n)}} p_u \\
&\leq \frac{1}{N^{(n)}} \sum_{u=1}^{N^{(n)}} (p_1 + \zeta_n) \\
&= \frac{1}{N^{(n)}} \cdot N^{(n)}(p_1 + \zeta_n) \\
&= p_1 + \zeta_n.
\end{aligned}$$

Similarly we can prove $\mathbb{E}\left[\overline{Y}\right] \geq p_1 - \zeta_n$. Since as n becomes large, $\zeta_n \longrightarrow 0$ and $p_1 \in (0, 1)$, we can conclude

$$\lim_{n\to\infty} \mathbb{E}\left[\overline{Y}\right] = p_1. \tag{2.10}$$

Also,

$$\begin{aligned}
Var\left(\overline{Y}\right) &= \frac{1}{\left(N^{(n)}\right)^2} \sum_{u=1}^{N^{(n)}} p_u \left(1 - p_u\right) \\
&\leq \frac{1}{(N^{(n)})^2} \sum_{u=1}^{N^{(n)}} \left(p_1 + \zeta_n\right)\left(1 - p_1 + \zeta_n\right) \\
&= \frac{1}{(N^{(n)})^2} \cdot N^{(n)} \left(p_1 + \zeta_n\right)\left(1 - p_1 + \zeta_n\right) \\
&= \frac{1}{N^{(n)}} \left(p_1 + \zeta_n\right)\left(1 - p_1 + \zeta_n\right).
\end{aligned}$$

Thus,

$$\lim_{n\to\infty} Var\left(\overline{Y}\right) = 0. \tag{2.11}$$

By using (2.10), (2.11), and Chebyshev's inequality, we can conclude

$$\overline{Y} \xrightarrow{d} p_1.$$

□

CHAPTER 3

PRIVACY OF INDEPENDENT USERS AGAINST STATISTICAL MATCHING: NON-ASYMPTOTIC RESULTS

3.1 Introduction

In Chapter 2, the concept of perfect privacy is defined and the limits of privacy are characterized. However, Chapter 2 limits their consideration to the asymptotic case. Here, we obtain the exact expressions for the discrete and finite case where user data samples are independent and identically distributed (*i.i.d.*) and independent of other users' data sets, while employing both anonymization and obfuscation techniques. Our results, while exact, are unwieldy. Similar to [62], the expression for the error probability could be used in asymptotic analyses to approach the problem from a different perspective from the information theoretic approach used in Chapter 2. In addition to its potential in asymptotic analyses, we demonstrate here how the results can be used to answer meaningful questions in the application. In particular, Chapter 2 indicates that, given enough obfuscation, the length m of the observed traces does not matter. Likewise, given a large enough m, obfuscation is not needed. And, conversely, if both are beneath their thresholds, a user does not have privacy. This gives the idea that the two methods work independently, and never need be employed in unison. Here, our expression for the finite case allow us to investigate whether this is true for smaller (practical) values of the number of users n and sequence length m.

The work presented in this chapter was published in [112].

Notation: In this chapter, $\mathbb{P}\left(X = x \middle| Y = y\right)$ is used for the conditional probability of $X = x$ given $Y = y$. When we write $\mathbb{P}\left(X \middle| Y\right)$, we are referring to a random variable that is defined as a function of Y.

3.2 System Model, Definitions, and Metrics

Consider a system with n users and denote $X_u(k)$ as a sample of the data of user u at time k, which we desire to protect from the adversary. In the discrete case, there is a countable number of possible states for each sample of each user's data. However, here we consider the binary case, where the data is restricted to $\{0, 1\}$. User u is distinguished by P_u the probability that $X_u(k) = 1$ for any k. Per Section 3.1, we assume the adversary knows P_u, $u = 1, 2, \cdots, n$, based on prior observations of the users, and it is this statistical knowledge that they will employ to identity users by the characteristics of their data traces. Finally, P_u, $u = 1, 2, \cdots, n$, are drawn independently from a distribution f_P.

As shown in Figure 3.1, we employ both anonymization and obfuscation techniques to protect the users' identities. In Figure 3.1, $Z_u(k)$ is the reported sample of the data of user u at time k, where $Z_u(k)$ has a Bernoulli distribution with the obfuscated probability of being in state 1 denoted as Q_u. $Y_u(k)$ is the data of user u at time k after applying both obfuscation and anonymization; $Y_u(k)$ has a Bernoulli distribution with the estimated probability of being in state 1 denoted as W_u.

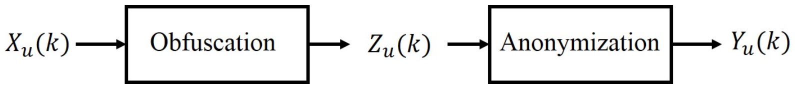


Figure 3.1: Applying obfuscation and anonymization techniques to users' data samples.

Obfuscation Model: The obfuscation is characterized by random variables, R_u, $u = 1, 2, \ldots, n$, which are drawn independently from a distribution f_R. The value of R_u is the probability that a sample of the data of user u is intentionally reported with error. Hence, the effect of the obfuscation is to alter the probability P_u, $u = 1, 2, \ldots, n$ of each user in a way that is unknown to the adversary, since the obfuscation is independent of all past activity of the user. For the binary case, where there are two states (state 0 and state 1) for a user's data pattern, we can write

$$Z_u(k) = \begin{cases} X_u(k), & \text{with probability of } 1 - R_u. \\ 1 - X_u(k), & \text{with probability of } R_u. \end{cases}$$

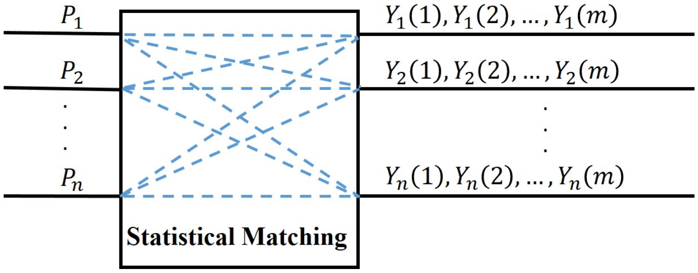
Anonymization Model: Anonymization is modeled by a random permutation Π such that for user u, the pseudonym of $\Pi(u)$ is assigned. The users' identities are permuted after each m samples, i.e., the observation sequences which the adversary uses to perform statistically matching are of length m. We can write

$$Y_u(k) = Z_{\Pi^{-1}(u)} \text{ and } Z_u(k) = Y_{\Pi(u)}.$$

The adversary attempts to identify the users based on the observations. Per above, we assume a powerful adversary who has complete statistical knowledge of the users' behavior, which means that they know P_u and their distribution f_P, for $u = 1, 2, \dots, n$. The adversary does not know the instantiation of R_u, $u = 1, 2, \dots, n$, or the permutation Π for each time period of length m.

The goal of the adversary is to correctly identify the users (i.e., figure out the instantiation of the permutation Π) based on their observation of $Y_{\Pi(u)}(k)$, $k = 1, 2, \dots, m$, $u = 1, 2, \dots, n$. We illustrate this in Figure 3.2, where the adversary tries to statistically match each P_u, $u = 1, 2, \dots, n$, to their corresponding observation sequences $Y_{\Pi(u)}$, $u = 1, 2, \dots, n$ in order to identify them.

Our metric is the adversary's probability of being correct, which is the probability that the adversary identifies the data of user u successfully.



P_1
P_2
P_n
$Y_1(1), Y_1(2), \dots, Y_1(m)$
$Y_2(1), Y_2(2), \dots, Y_2(m)$
$Y_n(1), Y_n(2), \dots, Y_n(m)$
Statistical Matching

Figure 3.2: The goal of the adversary: match each P_u of user u for $u = 1, 2, \dots, n$ to each observed sequences $Y_{\Pi(u)}(1), Y_{\Pi(u)}(2), \dots, Y_{\Pi(u)}(m)$ for $u = 1, 2, \dots, n$.

Here we assume the distribution f_P and the distribution f_R to be uniform. Note that the problem is still Bayesian because the adversary knows P_u and their distribution f_P, for $u = 1, 2, \cdots, n$.

3.3 Analytical and Numerical Results

3.3.1 Privacy with Anonymization

In this section, we consider the case where only anonymization is employed to provide user privacy. The identification problem can be formulated as a hypothesis testing problem, with the optimal test a straightforward adaptation of the work in [61]. This chapter provides an optimal hypothesis test in the case where the adversary has training sequences from the same group of users. Here, the optimal test can be obtained by replacing the empirical number of ones in [61] with the true (ensemble) values of $P_u, u = 1, 2, \cdots, n$. Thus, the optimal test is given by:

Theorem 6. The optimal hypothesis test in the case with binary observations and n users is given by: 1) Order (either descending or ascending) the data sequences by the number of ones they contain, and order $\{P_u, u = 1, 2, \cdots, n\}$; 2) match each data sequence to the P_u (and hence, the user) at the same position in these orders.

Let A_s, $s = 0, 1, \dots, \lceil \frac{n}{2} \rceil - 1$ be the event that: 1) exactly s of the users have $P_u \leq P_1$ but sum of observation sequence $\sum_{k=1}^{m} Y_{\Pi(u)}(k) \geq \sum_{k=1}^{m} Y_{\Pi(1)}(k)$ (we term this as "user moves from left to right"), and 2) exactly s users have $P_u \geq P_1$ but sum of observation sequence $\sum_{k=1}^{m} Y_{\Pi(u)}(k) \leq \sum_{k=1}^{m} Y_{\Pi(1)}(k)$, (we term this as "user moves from right to left") for $u = 1, 2, \ldots, n$. Given that $A_0, A_1, \cdots, A_{\lceil \frac{n}{2} \rceil - 1}$ are disjoint, the probability P_s that the adversary detects user 1 correctly is given by

$$P_s = \mathbb{P}\left(\bigcup_{s=0}^{\lceil \frac{n}{2} \rceil - 1} A_s \right) = \sum_{s=0}^{\lceil \frac{n}{2} \rceil - 1} \mathbb{P}(A_s).$$

We denote $W_u = \frac{\sum\limits_{k=1}^{m} Y_{\Pi(u)}(k)}{m}$, $u = 1, 2, \cdots, n$, as the estimation of P_u based on the observed sequence. Thus, in order to obtain $\mathbb{P}(A_s | P_1, W_1)$, we first consider the probability that a user moves from left to right, which we denote as $\mathbb{P}_{L \to R}(P_1 = p_1, W_1 = w_1)$, and the probability that a user moves from right to left, which we denote as $\mathbb{P}_{R \to L}(P_1 = p_1, W_1 = w_1)$. So we have,

$$\begin{aligned}
\mathbb{P}_{L \to R}\left(P_1 = p_1, W_1 = w_1\right) &= \mathbb{E}_{P_u}\Bigg[\mathbb{P}\left(\left\{\text{User } u \text{ moves to right}\right\} \Big| \left\{\text{User } u \text{ starts on left}\right\}\right) \\
&\qquad \cdot \mathbb{P}\left(\left\{\text{User } u \text{ starts on left}\right\} \Big| P_u, P_1 = p_1, W_1 = w_1\right)\Bigg] \\
&= \mathbb{E}_{P_u}\left[\sum_{l = \lceil w_1 \cdot m \rceil}^{m} \binom{m}{l} P_u^l \left(1 - P_u\right)^{m-1} I_{\{P_u \leq p_1\}}\right] \\
&= \int_0^{p_1} \sum_{l = \lceil w_1 \cdot m \rceil}^{m} \binom{m}{l} p_u^l \left(1 - p_u\right)^{m-1} dp_u.
\end{aligned}$$

Likewise,

$$\begin{aligned}
\mathbb{P}_{R \to L}\left(P_1 = p_1, W_1 = w_1\right) &= \mathbb{E}_{P_u}\Bigg[\mathbb{P}\left(\left\{\text{User } u \text{ moves to left}\right\} \Big| \left\{\text{User } u \text{ starts on right}\right\}\right) \\
&\qquad \cdot \mathbb{P}\left(\left\{\text{User } u \text{ starts on right}\right\} \Big| P_u, P_1 = p_1, W_1 = w_1\right)\Bigg] \\
&= \mathbb{E}_{P_u}\left[\sum_{l=0}^{\lfloor w_1 \cdot m \rfloor} \binom{m}{l} P_u^l \left(1 - P_u\right)^{m-1} I_{\{P_u \geq p_1\}}\right] \\
&= \int_{p_1}^{1} \sum_{l=0}^{\lfloor w_1 \cdot m \rfloor} \binom{m}{l} p_u^l \left(1 - p_u\right)^{m-1} dp_u.
\end{aligned}$$

Because a user's movement left-to-right or right-to-left is independent of other users when conditioned on P_1 and W_1, we obtain $\mathbb{P}(A_s|P_1,W_1)$ by employing a multinomial distribution with three categories. We denote N_1 as the number of users that move from left to right, N_2 as the number of users that move from right to left, and N_3 as the number of remaining users. Then,

$$\begin{aligned}\mathbb{P}(A_s|P_1,W_1) &= \mathbb{P}(N_1 = s, N_2 = s, N_3 = n-2s-1)\\ &= \frac{(n-1)!}{s!s!(n-2s-1)!} P_I^s P_{II}^s P_{III}^{n-2s-1},\end{aligned}$$

where $P_I = \mathbb{P}_{L\to R}(P_1 = p_1, W_1 = w_1)$, $P_{II} = \mathbb{P}_{R\to L}(P_1 = p_1, W_1 = w_1)$, and $P_{III} = 1 - \mathbb{P}_{L\to R}(P_1 = p_1, W_1 = w_1) - \mathbb{P}_{R\to L}(P_1 = p_1, W_1 = w_1)$.

Thus, the probability that the adversary successfully identifies user 1 is given by:

$$\begin{aligned}P_s =&\mathbb{E}_{P_1,W_1}\left[\sum_{s=0}^{\lceil\frac{n}{2}\rceil-1} \mathbb{P}(A_s|P_1,W_1)\right]\\ =& \int_0^1 \sum_{h=0}^{m} \sum_{s=0}^{\lceil\frac{n}{2}\rceil-1} \mathbb{P}(A_s|P_1,W_1)\, f_{P_1W_1}(p_1,h)dp_1. \qquad (3.1)\end{aligned}$$

where, noting p_1 is uniformly distributed on $[0,1]$,

$$\begin{aligned}f_{P_1W_1}(p_1,h) &= f_{W_1|P_1}(h|p_1)\cdot f_{P_1}(p_1)\\ &= \binom{m}{h} p_1^h (1-p_1)^{m-h}.\end{aligned}$$

To get some insight into the effect of anonymization on privacy, we show the probability of correct (P_s) in Figure 3.3, and compare the theoretical results in (3.1) with simulation results. As expected, the theoretical results match the simulation results. We can also notice that if we decrease the number m of observations per user, or increase the number n of users, the probability of correct decreases. This shows more users and a higher level of anonymization achieve more privacy, as expected.

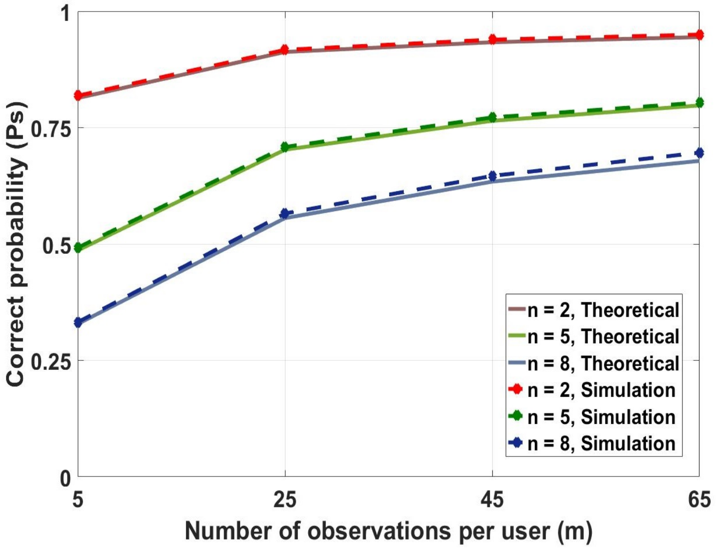


Figure 3.3: Comparison of simulation and theoretical results for correct probability (P_s) in identifying a given user when there are 2 users, 5 users, and 8 users in the case that only the anonymization technique is employed.

3.3.2 Privacy with Anonymization and Obfuscation

In this section, we employ both obfuscation and anonymization techniques to achieve privacy, and consider how these two techniques combine with each other to affect user privacy.

Recall that the obfuscation is characterized by a random variable R_u, $u = 1, 2, \cdots, n$, which given the probability that any data sample of user u is changed to a different data sample by obfuscation. We assume R_u is distributed uniformly over $[0, a]$, where a is noise level.

Let us define Q_u as the probability of $X_u(k) = 1$ after obfuscation; then we have

$$Q_u = P_u + R_u(1 - 2P_u)$$

Similar to the previous part, the probability that the adversary correctly identifies the data trace of user 1 is given by:

$$P_s = \mathbb{P}\left(\bigcup_{s=0}^{\lceil \frac{n}{2} \rceil - 1} A_s\right) = \sum_{s=0}^{\lceil \frac{n}{2} \rceil - 1} \mathbb{P}(A_s).$$

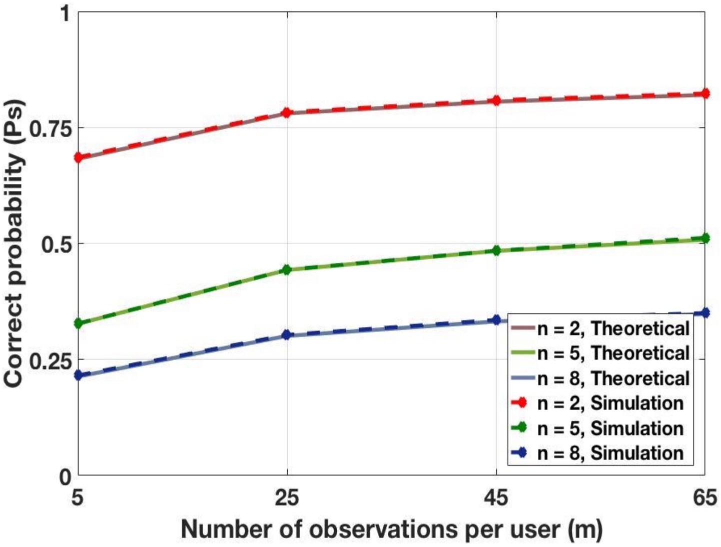


Figure 3.4: Comparison of simulation and theoretical results of the correct probability (P_s) in identifying a given user when there are 2 users, 5 users, and 8 users in the case that both obfuscation and anonymization techniques are employed. The noise level is fixed as $a = 0.5$.

To obtain $\mathbb{P}(A_s|P_1, R_1, W_1)$, consider the probability a user moves from left to right, which we denote as $\mathbb{P}_{L\to R}\left(P_1 = p_1, R_1 = r_1, W_1 = w_1\right)$ and the probability a user moves from right to left, which we denote as $\mathbb{P}_{R\to L}\left(P_1 = p_1, R_1 = r_1, W_1 = w_1\right)$. Now,

$$\begin{aligned}
&\mathbb{P}_{L\to R}\left(P_1 = p_1, R_1 = r_1, W_1 = w_1\right) = \\
&\mathbb{E}_{P_u, R_u}\left[\mathbb{P}\left(\left\{\text{User } u \text{ moves to right}\right\}\middle|\left\{\text{User } u \text{ starts on left}\right\}\right)\right. \\
&\left.\cdot\, \mathbb{P}\left(\left\{\text{User } u \text{ starts on left}\right\}\middle| P_u, R_u, P_1, R_1, W_1\right)\right] \\
&= \mathbb{E}_{P_u, R_u}\left[\sum_{l=\lceil w_1 \cdot m \rceil}^{m} \binom{m}{l} Q_u^l \left(1 - Q_u\right)^{m-1} I_{\{P_u \le p_1\}}\right] \\
&= \int_0^{p_1} \int_0^{a} \sum_{l=\lceil w_1 \cdot m \rceil}^{m} \binom{m}{l} q_u^l \left(1 - q_u\right)^{m-1} \cdot \left(\frac{1}{a}\right) dr_u dp_u.
\end{aligned}$$

Likewise,

$$\begin{aligned}
&\mathbb{P}_{R\to L}\left(P_1 = p_1, R_1 = r_1, W_1 = w_1\right) = \\
&\mathbb{E}_{P_u,R_u}\left[\mathbb{P}\left(\left\{\text{User } u \text{ moves to left}\right\}\middle|\left\{\text{User } u \text{ starts on right}\right\}\right)\right. \\
&\left.\cdot\, \mathbb{P}\left(\left\{\text{User } u \text{ starts on right}\right\}\middle| P_u, R_u, P_1, R_1, W_1\right)\right] \\
&= \mathbb{E}_{P_u,R_u}\left[\sum_{l=0}^{\lfloor w_1\cdot m\rfloor}\binom{m}{l}Q_u^l\left(1-Q_u\right)^{m-1} I_{\{P_u\geq p_1\}}\right] \\
&= \int_{p_1}^1\int_0^a\sum_{l=0}^{\lfloor w_1\cdot m\rfloor}\binom{m}{l}q_u^l\left(1-q_u\right)^{m-1}\cdot\left(\frac{1}{a}\right)dr_u dp_u,
\end{aligned}$$

As a result, for obtaining $\mathbb{P}\left(A_s|P_1, R_1, W_1\right)$, we write the multinomial distribution as

$$\begin{aligned}
\mathbb{P}\left(A_s|P_1, R_1, W_1\right) &= \mathbb{P}\left(N_1 = s, N_2 = s, N_3 = n-2s-1\right) \\
&= \frac{(n-1)!}{s!s!(n-2s-1)!}P_I^s P_{II}^s\cdot P_{III}^{n-2s-1},
\end{aligned}$$

where $P_I = \mathbb{P}_{L\to R}$, $P_{II} = \mathbb{P}_{R\to L}$, and $P_{III} = 1-\mathbb{P}_{L\to R}-\mathbb{P}_{R\to L}$.

Thus, the probability that the adversary successfully detects user 1 is given by

$$P_s = \mathbb{E}_{P_1,R_1,W_1}\left[\sum_{s=0}^{\lceil\frac{n}{2}\rceil-1}\mathbb{P}(A_s|P_1, R_1, W_1)\right].$$

Now we can conclude

$$P_s = \int_0^1\int_0^a\sum_{h=0}^{m}\sum_{s=0}^{\lceil\frac{n}{2}\rceil-1}\mathbb{P}\left(A_s|P_1, W_1\right) f_{P_1R_1W_1}(p_1, r_1, h)dr_1 dp_1, \tag{3.2}$$

where $f_{P_1R_1W_1}(p_1, r_1, h)$ is given by

$$\begin{aligned}
f_{P_1R_1W_1}(p_1, r_1, h) &= f_{W_1|R_1P_1}(h|r_1, p_1)f_{R_1|P_1}(r_1|p_1)f_{P_1}(p_1) \\
&= \binom{m}{h}p_1^h(1-p_1)^{m-h}\cdot\left(\frac{1}{a}\right).
\end{aligned}$$

Again, to get some insight of how anonymization and obfuscation combine to affect privacy, we provide numerical and simulation results in Figures 3.4 and 3.5. We compare the theoretical results in (3.2) with the simulation results, and, as expected, we see that the theoretical results match the simulation results.

In Figure 3.4, we show the correct probability (P_s) for different numbers of users (n) and length (m) of observation sequences, with a fixed noise level of $a = 0.5$. The figure implies that, similar to the case with only anonymization, if m decreases or n increases, the correct probability (P_s) decreases. In general, if we compare Figure 3.3 and Figure 3.4, we see that anonymization among with obfuscation leads to better results in preserving privacy, as expected from our intuition but in contrast to what is suggested by the asymptotic results of Chapter 2. We investigate this further in Figure 3.6 below.

In Figure 3.5, we fix $m = 5$ and show P_s for different n and a. We see that a higher level of noise results in a lower correct probability. It shows the degree to which a high level of obfuscation preserves privacy.

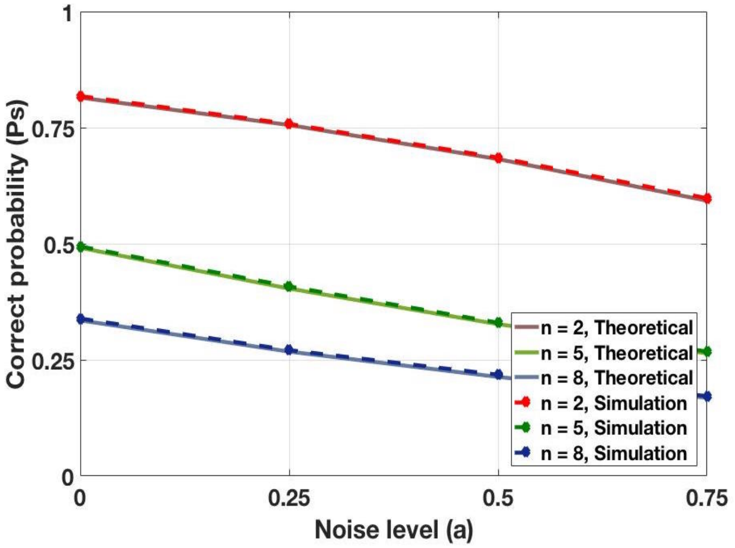


Figure 3.5: Comparison of simulation and theoretical results of the correct probability (P_s) in identifying a given user when there are 2 users, 5 users, and 8 users in the case that both obfuscation and anonymization techniques are employed. The length of the observation sequences is fixed as $m = 5$.

Finally, Figure 3.6 shows for small n and m, anonymization and obfuscation work together for preserving users' privacy. We see that when the anonymization level is not high enough (i.e. m is large) obfuscation helps in protecting user privacy (i.e. P_s decreases when a is large), and when the obfuscation level is not high enough (i.e. a is small), anonymization helps in protecting user privacy (i.e. P_s decreases when m is small). In fact, the sharp corner observed in the asymptotic case, which would suggest the center of the plot in Figure 3.6, would contain the corner of a box, is not evident. Instead, we see a smooth transition where the techniques can be used in conjunction when neither is sufficient by itself.

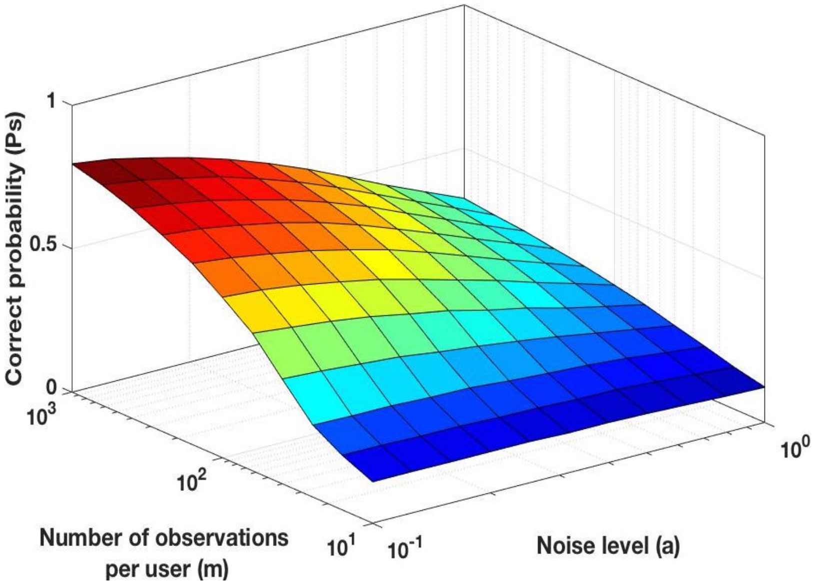


Figure 3.6: Simulation results for the correct probability (P_s) in identifying a given user vs. the number of observations per user (m) and noise level (a) for 10 users in the case that both obfuscation and anonymization techniques are employed.

CHAPTER 4

PRIVACY OF DEPENDENT USERS AGAINST STATISTICAL MATCHING

4.1 Introduction

Many modern applications provide an enhanced user experience by exploiting users' characteristics, including their past choices and present states. In particular, emerging Internet of Things (IoT) applications include smart homes, healthcare, and connected vehicles that intelligently tailor their performances to their users. For such applications to be able to provide their enhanced, user-tailored performances, they need to request their clients for potentially sensitive user information such as mobility behaviors and social preferences. Therefore, such applications trade off user privacy for enhanced utility. hence, questions arise about the degree to which user privacy is compromised in seeking an enhanced experience. Previous work [74] shows that even if users' data traces are anonymized before being provided to such applications, standard statistical matching techniques can be used to leak users' private information. Thus, privacy and security threats are a major obstacle to the wide adoption of IoT applications, as demonstrated by prior studies [3, 5, 27, 44, 47, 66, 84, 85, 87, 101, 115, 116, 118, 120, 122].

The bulk of previous work assumes independence between the traces of different users. [4, 22, 25, 68, 95, 126, 131] have mostly considered temporal and spatial dependency within data traces, but not cross-user dependency. In [4], an obfuscation technique is employed to achieve privacy; however, for continuous Location-Based Services (LBS) queries, there is often strong temporal dependency in the locations. Hence, [4] considers how dependency

The work presented in this chapter was published in [110, 114] and submitted to [108].

of the users' obfuscated data can impact privacy, and then employs an adaptive noise level to achieve more privacy while still maintaining an acceptable level of utility. Liu et al. [68] show that the spatiotemporal dependency between neighboring location sets can ruin the privacy achieved using a dummy-based location-privacy preserving mechanism (LPPM); to solve this problem, they propose a spatiotemporal dependency-aware privacy protection that perturbs the spatiotemporal dependency between neighboring locations. Zhang et al. [131] employ Protecting Location Privacy (PLP) against dependency-analysis attack in crowd sensing: the potential dependency between users' data is modeled, and the data is filtered to remove the samples that disclose the user's private data. In [126], locations of a single user are temporally dependent, and δ-location set based differential privacy is proposed to achieve location privacy at every timestamp. Finally, Song et al. [104] provide privacy when there is dependency within the data of a single user. In summary, previous studies do not consider dependency between users, which is the focus of this work. We argue that for many applications, there is dependency between the traces of different users. For example, friends tend to travel together or might meet at given places, hence introducing dependency between the traces of their location information. Several previous works [56, 57, 67, 78, 128, 130, 135] have considered cross-user dependency; however, this only has been for protecting queries on aggregated data, which is different than our application scenario.

We use the notion of "perfect privacy" and "no privacy", as introduced in Chapter 2, to evaluate the privacy of user traces. The "perfect privacy" notion provides an information-theoretic guarantee on privacy in the presence of a strong adversary who has complete knowledge on users' prior data traces. On the opposite extreme is the notion of 'no privacy". It means there exists an algorithm for the adversary to estimate the actual data points of users with diminishing error probability. In Chapter 2, we have derived the degree of user anonymization and data obfuscation required to obtain perfect privacy—assuming that the data traces of different users are *independent* across users. Particularly, we evaluated the case of independent and identically distributed (i.i.d.) samples from a given user and the case when there is temporal dependency within the trace of a given user (but independent across users). In this work, we expand our study to the case where there is dependency between the data traces of users. That is, we investigate how privacy is affected by the presence of dependency between the data traces of users when anonymization and obfuscation techniques are used. We show that dependency significantly reduces the privacy of users. Specifically, we show that the same anonymization and obfuscation levels that could produce perfect privacy for independent users result in no privacy for dependent users. Thus, in the presence of inter-user dependency, we need to employ much stronger anonymization and obfuscation compare to the case data traces of different users are independent.

We model dependency between user traces with an association graph, where the presence of an edge between the vertices corresponding to a pair of users indicates a non-zero dependency between their data traces. We employ standard concentration inequalities to demonstrate that the adversary can readily determine this association graph. Using this association graph and statistical data about the users, the adversary can attempt to identify users, and we demonstrate that this provides the adversary with a significant advantage versus the case when the data traces of different users are independent of one another. This suggests that, unless additional countermeasures are employed, the results of Chapter 2 for independent traces are optimistic when user traces are dependent. We next consider the effectiveness of countermeasures. First, we argue that adding independent obfuscation to user data points is often ineffective in improving the privacy of (dependent) users. Next, we demonstrate that, if users with dependent traces can jointly design their obfuscation, user privacy can be significantly improved.

A related but parallel approach to our study is graph alignment in which the edge set is sampled at random. Graph alignment is the problem of finding a matching between the vertices of the two graphs that matches, or aligns, many edges of the first graph with edges of the second graph. Shirani et. al. [92, 94] and Cullina et. al. [20] have done significant work on graph alignment. Although the graph alignment problem looks similar to our problem on the surface, there exist notable differences between the two. First, in Shirani et. al.'s work [92–94], graphs are generated using a model which is sampled at random from a probability distribution, while here the association graph is deterministic, as it is based on the dependency between data traces of users. Consequently, Shirani et. al. [92–94] used a completely different approach and solution to de-anonymize users. In other words, they have not used the probability distribution of the data traces of each user to break anonymization, while here the probability distribution of the data trace of each user is a key characteristic which helps the adversary to break users' privacy. Finally, Shirani et. al. [92, 94] considered discrete values for the correlation between users and used them to de-anonymize the graph, while here the correlation between users have continuous values and the adversary does not have access to the exact value of them.

[20,21,26] considered the graph alignment for two correlated graphs, while here we assume the adversary has the association graph and tries to reconstruct it from the anonymized and obfuscated data traces. Thus, in our work, the adversary has two identical graphs and their goal is to identify all of the users based on the observed data and their statistical knowledge of users. Also, Cullina et. al. [20] considered fractional matching, while here the adversary can identify not only all of the users but also the data points of each user at all time with small error probability. [48, 52, 83, 129] studied matching of non-identical pairs of correlated Erdös-Rényi graphs.

Also, graph isomorphism studied in [7,9,17,24] is an instance of the matching problem where the two graphs are identical copies of one another. [9] studied different algorithms such as maximum degree algorithms to match two identical graphs for the case where each edge of the graph has a fixed probability of being present or absent which is in the range of $\left[\omega\left(\log n/n^{\frac{1}{5}}\right), 1-\omega\left(\log n/n^{\frac{1}{5}}\right)\right]$, where n is the number of vertices in the graph. Here, the approach of our work is completely different, as the adversary uses probability distributions of users' data traces to reconstruct the association graph. After reconstruction of the association graph, the adversary uses the size of each disjoint group to identify all of the members.

In summary, although matching (alignment) between graphs can be considered as a part of our analysis, the analysis based on the users' data traces and the statistical knowledge of the adversary is a key part of this chapter which distinguishes it from previous works on graph alignment.

The rest of this chapter is organized as follows. In Section 4.2 we present the model and metrics considered in this work. In Sections 4.3 and 4.4, we show dependency between users' traces degrades privacy. In Section 4.5, we discuss how our methodology can be applied to a more general setting for the association graph. In Section 4.6, we propose a method to improve privacy in the case when there exists inter-user dependency.

4.2 System Model, Definitions, and Metrics

Here, we employ a similar framework to Chapter 2. The system has n users, and $X_u(k)$ is the data point of user u at time k. Our main goal is protecting $X_u(k)$ from a strong adversary who has full knowledge of the (unique) marginal probability distribution function of the data points of each user based on previous observations or other sources. In order to achieve data privacy for users, both anonymization and obfuscation techniques can be used as shown in Figure 4.1. In Figure 4.1, $Z_u(k)$ shows the (reported) data point of user u at time k after applying obfuscation, and $Y_u(k)$ shows the (reported) data point of user u at time k after applying anonymization to $Z_u(k)$. Let $m = m(n)$ be the number of data points after which the pseudonyms of users are changed using anonymization. To break obfuscation and anonymization, the adversary tries to estimate $X_u(k)$, $k = 1, 2, \cdots, m$, from m observations per user by matching the sequence of observations to the known statistical characteristics of the users. Let $\mathbf{X}_u$ be the $m \times 1$ vector containing the data points of user u, and $\mathbf{X}$ be the $m \times n$ matrix with the u^{th} column equal to $\mathbf{X}_u$:

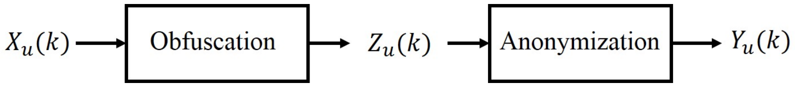


Figure 4.1: Applying obfuscation and anonymization techniques to the users' data points.

$$
\mathbf{X}_u = \begin{bmatrix} X_u(1) \\ X_u(2) \\ \vdots \\ X_u(m) \end{bmatrix}, \quad \mathbf{X} = \left[\mathbf{X}_1 \;\; \mathbf{X}_2 \;\; \cdots \;\; \mathbf{X}_n\right].
$$

Data Points Model: Here, we assume two different models for users' data points: in the first case, we assume the sequence of data for any individual user is modeled by i.i.d. which could apply directly to data that is sampled at a low rate. In addition, understanding the i.i.d. case can also be considered the first step toward understanding the more complicated case where there is temporal dependency. In the second case, we assume the data trace of any individual users is governed by Markov chain in which each sample of users' data is dependent over time.

We also assume users' data points can have one of r possible values $(0, 1, \cdots, r-1)$. Thus, according to a user-specific probability distribution $(\mathbf{p}_u)$, $X_u(k)$ is equal to a value in $\{0, 1, \cdots, r-1\}$ at any time. Note $p_u(i)$ is the probability of user u having the data value i, so

$$\mathbf{p}_u = \begin{bmatrix} p_u(1) \\ p_u(2) \\ \vdots \\ p_u(r-1) \end{bmatrix}, \text{ for each } u \in \{1, 2, \cdots, n\}.$$

We also assume $\mathbf{p}_u$'s are drawn independently from some continuous density function, $f_{\mathbf{P}}(\mathbf{p}_u)$, which has support on a subset of the $(0,1)^{r-1}$ hypercube. Note these user-specific probability distributions, i.e., $\mathbf{p}_u$'s, are known to the adversary and form the basis upon which they perform (statistical) matching.

Association Graph: An association graph or dependency graph is an undirected graph representing dependency of the data of users with each other. Let $G(\mathcal{V}, F)$ denote the association graph with set of nodes $\mathcal{V}$, ($|\mathcal{V}| = n$), and set of edges F. Two vertices (users) are connected if their data sets are dependent. More specifically,

- $(u, u') \notin F$ iff $\mathbb{I}(X_u(k); X_{u'}(k)) = 0$,
- $(u, u') \in F$ iff $\mathbb{I}(X_u(k); X_{u'}(k)) > 0$,

where $\mathbb{I}\left(X_u(k); X_{u'}(k)\right)$ is the mutual information between the k^{th} data point of user u and user u'[1].

Obfuscation Model: Obfuscation perturbs the users' data points [10, 39, 99]; in other words, the obfuscation can be viewed as passing data through a noisy channel. Normally, in such settings, each user has only limited knowledge of the characteristics of the overall population. Thus, usually, a simple distributed method in which the data points of each

[1] It is worth noting that the mechanism that determines the joint distribution of $X_u(k)$ and $X_{u'}(k)$ does not affect the results of this chapter as long as the marginal densities of $X_u(k)$'s (i.e., $\mathbf{p}_u$'s) are drawn independently from $f_{\mathbf{P}}(\mathbf{p}_u)$.

user are reported with error with a certain probability is employed [123]. Note that this probability itself is generated randomly for each user. Let $\mathbf{Z}_u$ be the vector that contains the obfuscated version of user u's data points, and $\mathbf{Z}$ be the collection of $\mathbf{Z}_u$ for all users,

$$\mathbf{Z}_u = \begin{bmatrix} Z_u(1) \\ \\ Z_u(2) \\ \\ \vdots \\ \\ Z_u(m) \end{bmatrix}, \quad \mathbf{Z} = [\mathbf{Z}_1 \ \mathbf{Z}_2 \ \cdots \ \mathbf{Z}_n].$$

Here, we define the *asymptotic noise level* for an obfuscation technique. Loosely speaking, the asymptotic noise level of obfuscation is the highest probable percentage of data points that are corrupted. More precisely, for a subset of users $\mathfrak{U}$, let $X_u(k)$ be the actual data point of user u at time k, $u \in \mathfrak{U}$, $k \in \{1, 2, \cdots, m\}$, and let $Z_u(k)$ be the obfuscated (noisy) version of $X_u(k)$. Define

$$A_m(u) = \frac{|\{k : Z_u(k) \neq X_u(k)\}|}{m}.$$

Then, the asymptotic noise level for user u is defined as follows:

$$a(u) = \inf\left\{\tau \geq 0 : \mathbb{P}\left(A_m(u) > \tau\right) \to 0 \text{ as } m \to \infty\right\}.$$

Also, define

$$A_m = \frac{\sum\limits_{u \in \mathfrak{U}} |\{k : Z_u(k) \neq X_u(k)\}|}{m|\mathfrak{U}|},$$

then, the asymptotic noise level for the entire dataset is

$$a = \inf\left\{\tau \geq 0 : \mathbb{P}\left(A_m > \tau\right) \to 0 \text{ as } m \to \infty\right\}.$$

Note that while the above definition is given for a general case required in Section 4.6, in practice we often use simple obfuscation techniques that employ i.i.d. noise sequences. Then, by the Strong Law of Large Number (SLLN),

$$\frac{|\{k : Z_u(k) \neq X_u(k)\}|}{m} \xrightarrow{\text{a.s.}} \mathbb{P}\left(Z_u(k) \neq X_u(k)\right),$$

and for any k,

$$a(u) = \mathbb{P}\left(Z_u(k) \neq X_u(k)\right).$$

Anonymization Model: In the anonymization technique, the identity of the users is perturbed [18, 33, 45, 71, 74, 96, 102]. Anonymization is modeled by a random permutation Π on the set of n users. Let $\mathbf{Y}_u$ be the vector which contains the anonymized version of $\mathbf{Z}_u$, and $\mathbf{Y}$ is the collection of $\mathbf{Y}_u$ for all users, thus

$$\begin{aligned}\mathbf{Y} &= \text{Perm}\left(\mathbf{Z}_1, \mathbf{Z}_2, \cdots, \mathbf{Z}_n; \Pi\right)\\ &= \left[\mathbf{Z}_{\Pi^{-1}(1)}\ \mathbf{Z}_{\Pi^{-1}(2)}\ \cdots\ \mathbf{Z}_{\Pi^{-1}(n)}\right]\\ &= \left[\mathbf{Y}_1\ \mathbf{Y}_2\ \cdots\ \mathbf{Y}_n\right],\end{aligned}$$

where Perm(. , Π) is the permutation operation with permutation function Π. As a result, $\mathbf{Y}_u = \mathbf{Z}_{\Pi^{-1}(u)}$ and $\mathbf{Y}_{\Pi(u)} = \mathbf{Z}_u$.

Adversary Model: We assume the adversary has full knowledge of the marginal probability distribution function of each of the users on $\{0, 1, \ldots, r-1\}$. As discussed in the data points models in succeeding sections, the parameters $\mathbf{p}_u$, $u = 1, 2, \cdots, n$ are drawn independently from a continuous density function, $f_{\mathbf{P}}(\mathbf{p}_u)$, which has support on a subset of a given hypercube. The density $f_{\mathbf{P}}(\mathbf{p}_u)$ might be unknown to the adversary, so all that is assumed here is that such a density exists. From the results, it will be evident that knowing or not knowing $f_{\mathbf{P}}(\mathbf{p}_u)$ does not change the results asymptotically.

The adversary knows the anonymization mechanism but does not know the realization of the random permutation. The adversary also knows the obfuscation mechanism but does not know the realization of the noise parameters. And finally, the adversary knows the association graph $G(\mathcal{V}, F)$, but does not necessarily know the exact nature of the dependency. That is, while the adversary knows the marginal distributions $X_u(k)$ as well as which pairs of users have strictly positive mutual information, they might not know the joint distributions or even the values of the mutual information $I(X_u(k); X_{u'}(k))$.

It is critical to note that the adversary does not have any other auxiliary information or side information about users' data.

We adopt the definitions of perfect privacy and no privacy from Chapter 2:

Definition 3. User u has *perfect privacy* at time k if and only if

$$\lim_{n\to\infty} \mathbb{I}\left(X_u(k); \mathbf{Y}\right) = 0,$$

where $\mathbb{I}\left(X_u(k); \mathbf{Y}\right)$ denotes the mutual information between the data point of user u at time k and the collection of the adversary's observations for all the users.

Definition 4. For an algorithm for the adversary that tries to estimate the actual data point of user u at time k, define the error probability as

$$\mathbb{P}_e(u,k) = \mathbb{P}\left(\widetilde{X_u(k)} \neq X_u(k)\right),$$

where $X_u(k)$ is the actual data point of user u at time k, $\widetilde{X_u(k)}$ is the adversary's estimated data point of user u at time k. Now, define $\mathcal{E}$ as the set of all possible adversary's estimators. Then, user u has *no privacy* at time k, if and only if,

$$\mathbb{P}_e^*(u,k) = \lim_{n\to\infty} \inf_{\mathcal{E}} \mathbb{P}\left(\widetilde{X_u(k)} \neq X_u(k)\right) \to 0.$$

Hence, a user has *no privacy* if there exists an algorithm for the adversary to estimate $X_u(k)$ with diminishing error probability as n goes to infinity.

Discussion 1: The studied anonymization and obfuscation mechanisms improve user privacy at the cost of user utility. An anonymization mechanism works by frequently changing the pseudonym mappings of users to reduce the length of time series that can be exploited by statistical analysis. However, such frequent changes may also degrade the usability of the underlying application by concealing the temporal relation between a user's data points, e.g., for a dining recommendation system that makes suggestions based on the dining history of its users. On the other hand, obfuscation mechanisms work by adding noise to users' collected data, e.g., location information. The added noise may also degrade the utility of the system. In this work, our goal is studying the level of anonymization and obfuscation one should employ to ensure privacy with the minimum loss in utility. In other words, we derive the optimal frequency of changing user pseudonyms during anonymization, and the optimal extent of noise added by an obfuscation mechanism while guaranteeing privacy.

However, like similar works in privacy [18,33,45,71,74,118], we consider the quantification of utility orthogonal to our privacy evaluations for two reasons: (1) the implications of our PPMs on utility do not impact our privacy analysis, and (2) unlike privacy, the desired level of utility is application specific.

Discussion 2: Note that there are two kinds of dependency:

- Intra-user dependency: In this case, there is temporal and spatial dependency within data traces of one user. For example, when the data trace of a user is governed by a Markov chain model, the Markov chain characterizes temporal intra-user dependency. Thus, the adversary can benefit from this dependency and break the users' privacy. According to the results obtained in [111], when there are a large number of users in the setting ($n \to \infty$), and data traces of the users are governed by i.i.d. statistics with r possible values for each data point, users have no privacy if and only if the number of adversary's observations per user (m) is significantly larger than $n^{\frac{2}{r-1}}$ and the amount of noise level (a_n) is significantly smaller than $n^{-\frac{1}{r-1}}$; however, if the data trace of users is governed by an irreducible and aperiodic Markov chains with r states and $|E|$ edges, users have no privacy if and only if the number of adversary's observations per user (m) is significantly larger than $n^{\frac{2}{|E|-r}}$ and the amount of noise level (a_n) is significantly smaller than $n^{-\frac{1}{|E|-r}}$. Most of the previous work [4, 22, 25, 68, 95, 126, 131] that considers intra-user dependency assumes independence between the traces of different users, which is different from our work as described below.

- Inter-user dependency: Here, there exists dependency between the traces of different users. This is the main focus of our work. First, we demonstrate that the adversary can readily identify the association graph of the obfuscated and anonymized version of the data, revealing which user data traces are dependent. Next, we demonstrate that the adversary can use this association graph along with their statistical knowledge and the observed obfuscated and anonymized sequences to break user privacy with significantly shorter traces than in the case of independent users, and that obfuscating data traces independently across users is often insufficient to remedy such leakage.

Discussion 3: The general models of multi-user in classical information theory assume a fixed number of users and the fundamental limits of communication systems are characterized by studying the asymptotic limits of infinite coding blocklength [41, 43, 63, 119]. However, the emerging Internet of Things enables an ever-increasing number of users to share and access information on a large scale, i.e., applications, such as ride sharing and dining recommendation applications, the number of users is large. Thus, the number of users is allowed to grow with the blocklength [13, 14, 42], and our goal is for the asymptotic results to provide a good insight to the performance of the privacy-preserving mechanisms for these applications. Moreover, both of the privacy definitions given above (perfect privacy and no privacy) are asymptotic in the number of users ($n \to \infty$), which allows us to find clean analytical results for the fundamental limits.

4.3 Impact of Dependency on Privacy Using Anonymization

In this section, we consider only anonymization and thus the obfuscation block in Figure 4.1 is not present. In this case, the adversary's observation $\mathbf{Y}$ is the anonymized version of $\mathbf{X}$; thus

$$\begin{aligned}\mathbf{Y} &= \text{Perm}\left(\mathbf{X}_1, \mathbf{X}_2, \cdots, \mathbf{X}_n; \Pi\right)\\ &= \left[\mathbf{X}_{\Pi^{-1}(1)} \ \mathbf{X}_{\Pi^{-1}(2)} \ \cdots \ \mathbf{X}_{\Pi^{-1}(n)}\right]\\ &= \left[\mathbf{Y}_1 \ \mathbf{Y}_2 \ \cdots \ \mathbf{Y}_n\right].\end{aligned}$$

4.3.1 r-State i.i.d. Model

There is potentially dependency between the data of different users, but we assume here that the sequence of data for any individual user is i.i.d.. We also assume users' data points can have r possibilities $(0, 1, \cdots, r-1)$, and $p_u(i)$ is the probability of user u having the data value i, i.e., $p_u(i) = \mathbb{P}\left(X_u(k) = i\right)$, for $k = 1, 2, \cdots, m$. We define the vectors $\mathbf{p}_u$ and $\mathbf{p}$ as

$$\mathbf{p}_u = \begin{bmatrix} p_u(1) \\ p_u(2) \\ \vdots \\ p_u(r-1) \end{bmatrix}, \quad \mathbf{p} = \left[\mathbf{p}_1 \ \mathbf{p}_2 \ \cdots \ \mathbf{p}_n\right].$$

We also assume $\mathbf{p}_u$'s are drawn independently from some continuous density function, $f_{\mathbf{P}}(\mathbf{p}_u)$, which has support on a subset of the $(0,1)^{r-1}$ hypercube. In particular, define the range of the distribution as

$$\mathcal{R}_{\mathbf{P}} = \left\{(x_1, x_2, \cdots, x_{r-1}) \in (0,1)^{r-1} : x_i > 0, x_1 + x_2 + \cdots + x_{r-1} < 1\right\},$$

then, we assume there are $\delta_1, \delta_2 > 0$ such that:

$$\begin{cases} \delta_1 \leq f_{\mathbf{P}}(\mathbf{p}_u) \leq \delta_2, & \mathbf{p}_u \in \mathcal{R}_{\mathbf{P}}. \\ f_{\mathbf{P}}(\mathbf{p}_u) = 0, & \mathbf{p}_u \notin \mathcal{R}_{\mathbf{P}}. \end{cases}$$

The adversary knows the values of $\mathbf{p}_u$, $u = 1, 2, \cdots, n$, and uses this knowledge to match the observed traces to the users. We will use capital letters (i.e., $\mathbf{P}_u$) when we are referring to the random variable, and use lower case (i.e., $\mathbf{p}_u$) to refer to the realization of $\mathbf{P}_u$.

A vector containing the permutation of those probabilities after anonymization is

$$\begin{aligned} \mathbf{W} &= \text{Perm}\left(\mathbf{P}_1, \mathbf{P}_2, \cdots, \mathbf{P}_n; \Pi\right) \\ &= \left[\mathbf{P}_{\Pi^{-1}(1)} \;\; \mathbf{P}_{\Pi^{-1}(2)} \;\; \cdots \;\; \mathbf{P}_{\Pi^{-1}(n)}\right] \\ &= \left[\mathbf{W}_1 \;\; \mathbf{W}_2 \;\; \cdots \;\; \mathbf{W}_n\right], \end{aligned}$$

where $\mathbf{W}_u = \mathbf{P}_{\Pi^{-1}(u)}$ and $\mathbf{W}_{\Pi(u)} = \mathbf{P}_u$.

In this case, we can say:

- $(u, u') \notin F$ iff for all $i, j \in \{0, 1, \cdots, r-1\}$, $p_{uu'}(i, j) = p_u(i) p_{u'}(j)$,
- $(u, u') \in F$ iff for at least one pair of $i, j \in \{0, 1, \cdots, r-1\}$, $p_{uu'}(i, j) \neq p_u(i) p_{u'}(j)$,

where $p_{uu'}(i, j) = \mathbb{P}\left(X_u(k) = i, X_{u'}(k) = j\right)$, $p_u(i) = \mathbb{P}\left(X_u(k) = i\right)$, and $p_{u'}(j) = \mathbb{P}\left(X_{u'}(k) = j\right)$. Note that the adversary knows the association graph $G(\mathcal{V}, F)$, but does not necessarily know the joint probability distribution for each specific $(u, u') \in F$. The adversary observes the anonymized version of users' data traces and combines them with their full knowledge of the marginal probability distribution of each of the users and the structure of the whole association graph to break users' privacy with arbitrarily small error probability.

In the first step, we show that the adversary can reliably reconstruct the entire association graph for *the anonymized version of the data* (i.e., the observed data traces) with relatively few observations.

Lemma 7. Consider a general association graph $G(\mathcal{V}, F)$. If the adversary obtains $m = (\log n)^3$ anonymized observations per user, they can construct $\widetilde{G} = \widetilde{G}(\widetilde{\mathcal{V}}, \widetilde{F})$, where $\widetilde{\mathcal{V}} = \{\Pi(u) : u \in \mathcal{V}\} = \mathcal{V}$, such that with high probability, for all $u, u' \in \mathcal{V}$; $(u, u') \in F$ iff $(\Pi(u), \Pi(u')) \in \widetilde{F}$. We write this statement as $\mathbb{P}(\widetilde{G} \simeq G) \to 1$, i.e., Graph G and Graph $\widetilde{G}$ are isomorphic with high probability.

Proof. For $u, u' \in \{1, 2, \cdots, n\}$, we normally write $v = \Pi(u)$ and $v' = \Pi(u')$. We provide an algorithm for the adversary that with high probability obtains all edges of F correctly. First, for all $v, v' \in \{1, 2, \cdots, n\}$, and all $i, j \in \{0, 1, \cdots, r-1\}$ the adversary computes $\widetilde{p_{vv'}(i,j)}$, $\widetilde{p_v(i)}$, and $\widetilde{p_{v'}(j)}$ as follow:

$$\widetilde{p_{vv'}(i,j)} = \frac{|\{k : Y_v(k) = i, Y_{v'}(k) = j\}|}{m} = \frac{\widehat{M}_{vv'}(i,j)}{m}, \tag{4.1}$$

$$\widetilde{p_v(i)} = \frac{|\{k : Y_v(k) = i\}|}{m} = \frac{\widehat{M}_v(i)}{m}, \tag{4.2}$$

$$\widetilde{p_{v'}(j)} = \frac{|\{k : Y_{v'}(k) = j\}|}{m} = \frac{\widehat{M}_{v'}(j)}{m}, \tag{4.3}$$

where

$$\widehat{M}_{vv'}(i,j) = |\{k : Y_v(k) = i, Y_{v'}(k) = j\}|.$$

$$\widehat{M}_v(i) = |\{k : Y_v(k) = i\}|.$$

$$\widehat{M}_{v'}(j) = |\{k : Y_{v'}(k) = j\}|.$$

After observing $m = (\log n)^3$ data points per user and computing the above expressions, the adversary constructs $\widetilde{G}$ in the following way:

- If $\left| \frac{\widehat{M}_{vv'}(i,j)}{m} - \frac{\widehat{M}_v(i)}{m} \frac{\widehat{M}_{v'}(j)}{m} \right| \leq m^{-\frac{1}{5}}$ for all $i, j \in \{0, 1, \cdots, r-1\}$, then $(v, v') \notin \widetilde{F}$.

- If $\left|\frac{\widehat{M}_{vv'}(i,j)}{m} - \frac{\widehat{M}_v(i)}{m}\frac{\widehat{M}_{v'}(j)}{m}\right| \geq m^{-\frac{1}{5}}$ for at least one pair of $i, j \in \{0, 1, \cdots, r-1\}$, then $(v, v') \in \widetilde{F}$.

We show the above method yields $\mathbb{P}(\widetilde{G} \simeq G) \to 1$ as $n \to \infty$, as follows. Note

$$\widehat{M}_{vv'}(i,j) \sim \text{Binomial}(m, w_{vv'}(i,j)),$$

$$\widehat{M}_v(i) \sim \text{Binomial}(m, w_v(i)),$$

$$\widehat{M}_{v'}(j) \sim \text{Binomial}(m, w_{v'}(j)),$$

where $w_{vv'}(i,j) = \mathbb{P}(Y_v(k) = i, Y_{v'}(k) = j) = p_{\Pi^{-1}(v)\Pi^{-1}(v')}(i,j)$, $w_v(i) = \mathbb{P}(Y_v(k) = i) = p_{\Pi^{-1}(v)}(i)$, and $w_{v'}(j) = \mathbb{P}(Y_{v'}(k) = j) = p_{\Pi^{-1}(v')}(j)$. Now, for all $v, v' \in \{1, 2, \cdots, n\}$ and all $i, j \in \{0, 1, \cdots, r-1\}$, define

$$\mathcal{J}_{vv'}(i,j) = \left\{\left|\frac{M_{vv'}(i,j)}{m} - w_{vv'}(i,j)\right| \geq m^{-\frac{1}{4}}\right\},$$

then, for all $v, v' \in \{1, 2, \cdots, n\}$ and all $i, j \in \{0, 1, \cdots, r-1\}$, the Chernoff bound yields

$$\mathbb{P}\left(\mathcal{J}_{vv'}(i,j)\right) \leq 2e^{-\frac{\sqrt{m}}{3w_{vv'}(i,j)}} \leq 2e^{-\frac{\sqrt{m}}{3}}.$$

Similarly, for all $v, v' \in \{1, 2, \cdots, n\}$ and all $i, j \in \{0, 1, \cdots, r-1\}$, define

$$\mathcal{J}_v(i) = \left\{\left|\frac{M_v(i)}{m} - w_v(i)\right| \geq m^{-\frac{1}{4}}\right\},$$

$$\mathcal{J}_{v'}(j) = \left\{\left|\frac{M_{v'}(j)}{m} - w_{v'}(j)\right| \geq m^{-\frac{1}{4}}\right\},$$

then, the Chernoff bound yields,

$$\mathbb{P}\left(\mathcal{J}_v(i)\right) \leq 2e^{-\frac{\sqrt{m}}{3}},$$

$$\mathbb{P}\left(\mathcal{J}_{v'}(j)\right) \le 2e^{-\frac{\sqrt{m}}{3}},$$

Now, by employing a union bound, for all $v, v' \in \{1, 2, \cdots, n\}$ and all $i, j \in \{0, 1, \cdots, r-1\}$, we have

$$\mathbb{P}\left(\mathcal{J}_{vv'}(i,j) \cup \mathcal{J}_{v}(i) \cup \mathcal{J}_{v'}(j)\right) \le 2\left(e^{-\frac{\sqrt{m}}{3}} + e^{-\frac{\sqrt{m}}{3}} + e^{-\frac{\sqrt{m}}{3}}\right) = 6e^{-\frac{\sqrt{m}}{3}}.$$

Then, by employing a union bound again,

$$\begin{aligned}\mathbb{P}\left(\bigcup_{v=1}^{n}\bigcup_{v'=1}^{n}\bigcup_{i=0}^{r-1}\bigcup_{j=0}^{r-1}\{\mathcal{J}_{vv'}(i,j) \cup \mathcal{J}_{v}(i) \cup \mathcal{J}_{v'}(j)\}\right) &\le \sum_{v=1}^{n}\sum_{v'=1}^{n}\sum_{i=0}^{r-1}\sum_{j=0}^{r-1} 6e^{-\frac{\sqrt{m}}{3}} \\ &= 6n^2r^2e^{-\frac{\sqrt{m}}{3}} \\ &= 6r^2 \exp\left\{2\log n - \frac{(\log n)^{\frac{3}{2}}}{3}\right\} \to 0,\end{aligned} \tag{4.4}$$

as $n \to \infty$. Thus, (4.4) yields that with high probability, for all $v, v' \in \{1, 2, \cdots, n\}$ and all $i, j \in \{0, 1, \cdots, r-1\}$, we have

$$0 \le mw_{vv'}(i,j) - m^{\frac{3}{4}} \le \widehat{M}_{vv'}(i,j) \le mw_{vv'}(i,j) + m^{\frac{3}{4}}. \tag{4.5}$$

$$0 \le mw_{v}(i) - m^{\frac{3}{4}} \le \widehat{M}_{v}(i) \le mw_{v}(i) + m^{\frac{3}{4}}. \tag{4.6}$$

$$0 \le mw_{v'}(j) - m^{\frac{3}{4}} \le \widehat{M}_{v'}(j) \le mw_{v}(j) + m^{\frac{3}{4}}. \tag{4.7}$$

Let us define event $A_{vv'}(i,j)$ as the event that (4.5), (4.6), and (4.7) are all valid, thus, as shown in (4.4), we have

$$\mathbb{P}\left(\bigcap_{v=1}^{n}\bigcap_{v'=1}^{n}\bigcap_{i=0}^{r-1}\bigcap_{j=0}^{r-1}\{A_{vv'}(i,j)\}\right) \to 1, \tag{4.8}$$

as $n \to \infty$. Now, if $A_{vv'}(i,j)$ is true for some $v, v' \in \{1, 2, \cdots, n\}$ and some $i, j \in \{0, 1, \cdots, r-1\}$, we have

$$\begin{aligned}\frac{\widehat{M}_{vv'}(i,j)}{m} - \frac{\widehat{M}_{v}(i)}{m}\frac{\widehat{M}_{v'}(j)}{m} &\leq \frac{mw_{vv'}(i,j) + m^{\frac{3}{4}}}{m} - \frac{mw_{v}(i) - m^{\frac{3}{4}}}{m}\frac{mw_{v'}(i) - m^{\frac{3}{4}}}{m} \\ &= w_{vv'}(i,j) - w_{v}(i)w_{v'}(j) + m^{-\frac{1}{4}} + (w_{v}(i) + w_{v'}(j))m^{-\frac{1}{4}} - m^{-\frac{1}{2}} \\ &\leq w_{vv'}(i,j) - w_{v}(i)w_{v'}(j) + m^{-\frac{1}{4}} + (w_{v}(i) + w_{v'}(j))m^{-\frac{1}{4}} + m^{-\frac{1}{2}}.\end{aligned} \tag{4.9}$$

Similarly,

$$\begin{aligned}\frac{\widehat{M}_{vv'}(i,j)}{m} - \frac{\widehat{M}_{v}(i)}{m}\frac{\widehat{M}_{v'}(j)}{m} &\geq \frac{mw_{vv'}(i,j) - m^{\frac{3}{4}}}{m} - \frac{mw_{v}(i) + m^{\frac{3}{4}}}{m}\frac{mw_{v'}(i) + m^{\frac{3}{4}}}{m} \\ &= w_{vv'}(i,j) - w_{v}(i)w_{v'}(j) - m^{-\frac{1}{4}} - (w_{v}(i) + w_{v'}(j))m^{-\frac{1}{4}} - m^{-\frac{1}{2}}.\end{aligned} \tag{4.10}$$

Thus, by using (4.9) and (4.10), we have

$$\left|\left(\frac{\widehat{M}_{vv'}(i,j)}{m} - \frac{\widehat{M}_{v}(i)}{m}\frac{\widehat{M}_{v'}(j)}{m}\right) - (w_{vv'}(i,j) - w_{v}(i)w_{v'}(j))\right| \leq (1 + w_{v}(i) + w_{v'}(j))m^{-\frac{1}{4}} + m^{-\frac{1}{2}}. \tag{4.11}$$

Let us define event $B_{vv'}(i,j)$ as the event that (4.11) is valid for v, v', i, and j. We have shown, for all $v, v' \in \{1, 2, \cdots, n\}$ and all $i, j \in \{0, 1, \cdots, r-1\}$, $A_{vv'}(i,j) \subseteq B_{vv'}(i,j)$, thus

$$\left\{\bigcap_{v=1}^{n}\bigcap_{v'=1}^{n}\bigcap_{i=0}^{r-1}\bigcap_{j=0}^{r-1}\{A_{vv'}(i,j)\}\right\} \subseteq \left\{\bigcap_{v=1}^{n}\bigcap_{v'=1}^{n}\bigcap_{i=0}^{r-1}\bigcap_{j=0}^{r-1}\{B_{vv'}(i,j)\}\right\},$$

and as a result,

$$\mathbb{P}\left(\bigcap_{v=1}^{n}\bigcap_{v'=1}^{n}\bigcap_{i=0}^{r-1}\bigcap_{j=0}^{r-1}\{B_{vv'}(i,j)\}\right) \geq \mathbb{P}\left(\bigcap_{v=1}^{n}\bigcap_{v'=1}^{n}\bigcap_{i=0}^{r-1}\bigcap_{j=0}^{r-1}\{A_{vv'}(i,j)\}\right).$$

Thus, by using (4.8), we have

$$\mathbb{P}\left(\bigcap_{v=1}^{n}\bigcap_{v'=1}^{n}\bigcap_{i=0}^{r-1}\bigcap_{j=0}^{r-1}\{B_{vv'}(i,j)\}\right) \to 1,$$

as $n \to \infty$. Hence, with high probability, for all $v, v' \in \{1, 2, \cdots, n\}$ and all $i, j \in \{0, 1, \cdots, r-1\}$, we have

$$\left|\left(\frac{\widehat{M}_{vv'}(i,j)}{m} - \frac{\widehat{M}_v(i)}{m}\frac{\widehat{M}_{v'}(j)}{m}\right) - (w_{vv'}(i,j) - w_v(i)w_{v'}(j))\right| \leq (1 + w_v(i) + w_{v'}(j))m^{-\frac{1}{4}} + m^{-\frac{1}{2}}. \tag{4.12}$$

Now, if $(u, u') \notin F$, then for all $i, j \in \{0, 1, \cdots, r-1\}$, we have $p_{uu'}(i,j) - p_u(i)p_{u'}(j) = 0$, and as a result, $w_{vv'}(i,j) - w_v(i)w_{v'}(j) = 0$. Thus, by using (4.12), we have

$$\left|\frac{\widehat{M}_{vv'}(i,j)}{m} - \frac{\widehat{M}_v(i)}{m}\frac{\widehat{M}_{v'}(j)}{m}\right| \leq (1 + w_v(i) + w_{v'}(j))m^{-\frac{1}{4}} + m^{-\frac{1}{2}},$$

and as a result, as $m \to \infty$,

$$\left|\frac{\widehat{M}_{vv'}(i,j)}{m} - \frac{\widehat{M}_v(i)}{m}\frac{\widehat{M}_{v'}(j)}{m}\right| \leq m^{-\frac{1}{5}}.$$

Thus, we can conclude, $(v, v') \notin \widetilde{F}$, and in other words, $(\Pi(u), \Pi(u')) \notin \widetilde{F}$. This is true with high probability, for all $u, u' \in \{1, 2, \cdots, n\}$ where $(u, u') \notin F$.

Similarly, if $(u, u') \in F$, there exists at least one pair of $i, j \in \{0, 1, \cdots, r-1\}$ with $p_{uu'}(i,j) - p_u(i)p_{u'}(j) \geq \epsilon - m^{-\frac{1}{4}}$ for a fixed value of ϵ. Thus, there exists at least one pair of $i, j \in \{0, 1, \cdots, r-1\}$ with $w_{vv'}(i,j) - w_v(i)w_{v'}(j) \geq \epsilon - m^{-\frac{1}{4}}$. As a result, by using (4.12), for large enough m, we have

$$\left|\frac{\widehat{M}_{vv'}(i,j)}{m} - \frac{\widehat{M}_v(i)}{m}\frac{\widehat{M}_{v'}(j)}{m}\right| \geq m^{-\frac{1}{5}}.$$

Thus, we can conclude, $(v, v') \in \widetilde{F}$, and in other words, $(\Pi(u), \Pi(u')) \in \widetilde{F}$. Again, this is true with high probability, for all $u, u' \in \{1, 2, \cdots, n\}$ where $(u, u') \in F$.

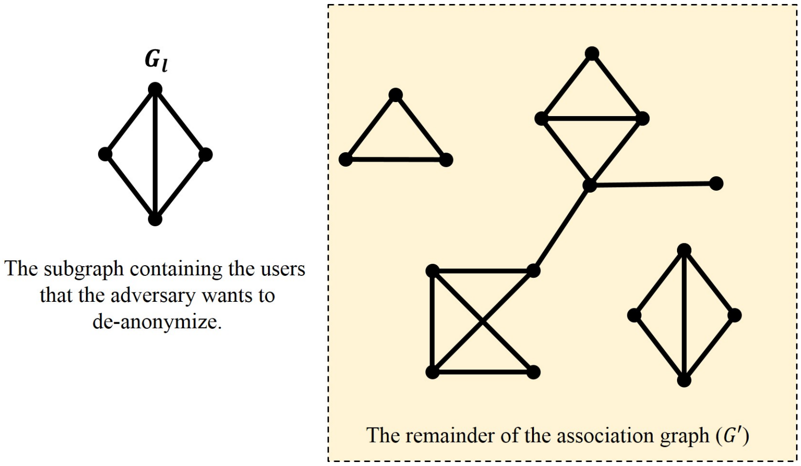

G_l
The subgraph containing the users that the adversary wants to de-anonymize.
The remainder of the association graph (G')

Figure 4.2: The structure of the association graph (G): Group l with s_l vertices is disjoint from the reminder of the association graph (G').

Now, we can conclude, for large enough n, we have $\mathbb{P}\left(\widetilde{G} \simeq G\right) \to 1$, so the adversary can reconstruct the association graph of the anonymized version of the data with an arbitrarily small error probability. Note that reconstruction of the association graph does not require the adversary's knowledge about user statistics (i.e., the values of $\mathbf{p}_u$'s). □

The structure of the association graph (G) can leak a lot of information. For the rest of this section, we consider a graph structure shown in Figure 4.2. In this structure, G_l, the subgraph consisting of the users the adversary wants to de-anonymize, has s_l vertices and is disjoint from the reminder of the association graph. So, we can write $G_l(\mathcal{V}_l, F_l)$, where $|\mathcal{V}_l| = s_l$. Note that we assume s_l is finite. In particular, the subgraph G_l can be thought of as a group of "friends" or "associates" such that their data sets are dependent. In Section 4.5, we discuss how our methodology can be applied to the settings where the subgraph G_l is not disjoint from the reminder of the graph (G') [23, 32, 35, 37, 38, 53, 75, 77, 100, 125].

The following theorem states that if the number of observations per user (m) is significantly larger than $n^{\frac{2}{s(r-1)}+\alpha}$ in the r-state model, where s is the size of a group, then the adversary can successfully de-anonymize the users in that group.

Theorem 7. For the above r-state model, if $\mathbf{Y}$ is the anonymized version of $\mathbf{X}$ as defined above, the size of the group including user 1 is s, and

- $m = \Omega\left(n^{\frac{2}{s(r-1)}+\alpha}\right)$, for any $\alpha > 0$;

then, user 1 has no privacy at time k.

Discussion 4: It is insightful to compare this result to [73, Theorem 2], where it is stated that if the users are not dependent, then all users have perfect privacy as long as the number of adversary's observations per user (m) is smaller than $O(n^{\frac{2}{r-1}-\alpha})$. Here, Theorem 7 states that with much smaller m, the adversary can de-anonymize the users. Therefore, we see that dependency can significantly reduce the privacy of users.

Proof of Theorem 7:

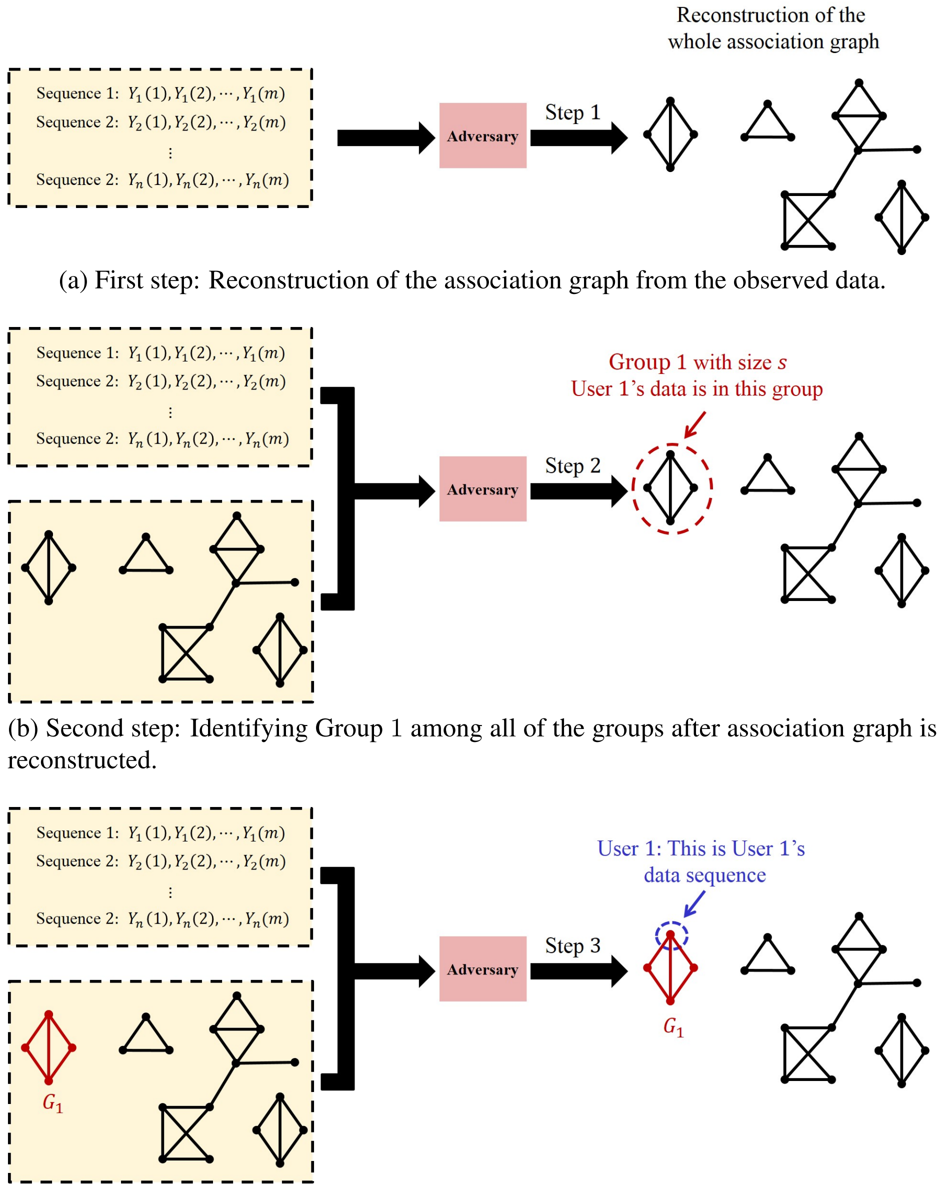
Proof. As shown in Figure 4.3, the proof of Theorem 7 consists of three parts:

- **First Step:** Showing the adversary can reconstruct the association graph of the anonymized version of the data with an arbitrarily small error probability (as shown in Figure 4.3a).

- **Second Step:** Showing the adversary can uniquely identify Group 1 with an arbitrarily small error probability (as shown in Figure 4.3b).

- **Third Step:** Showing the adversary can individually identify all the members within Group 1 with an arbitrarily small error probability (as shown in Figure 4.3c).

The first part of the proof exploits the fact that the adversary can readily reconstruct the association graph of the anonymized data in $m = (\log n)^3$. It is the second and third parts that give rise to the condition $m = \Omega\left(n^{\frac{2}{s(r-1)}+\alpha}\right)$, and it is in the second part where we see the mechanism for the speed-up of the adversary's algorithm relative to the case where user traces are independent. In particular, due to the dependence between users breaking them into groups, the key search for the adversary now involves finding a set of


Reconstruction of the whole association graph
Sequence 1: $Y_1(1), Y_1(2), \cdots, Y_1(m)$
Sequence 2: $Y_2(1), Y_2(2), \cdots, Y_2(m)$
⋮
Sequence 2: $Y_n(1), Y_n(2), \cdots, Y_n(m)$
Adversary
Step 1
Group 1 with size s
User 1's data is in this group
Step 2
User 1: This is User 1's data sequence
Step 3
G_1

(a) First step: Reconstruction of the association graph from the observed data.

(b) Second step: Identifying Group 1 among all of the groups after association graph is reconstructed.

(c) Third step: Identifying user 1 among all of the members of Group 1 after Group 1 is uniquely identified.

Figure 4.3: The algorithm of the adversary to estimate data points of user 1 with vanishing error probability.

users corresponding to a length-s vector of probabilities rather than searching for a single user associated with a given probability.

First step: Reconstruction of the association graph: In this step, we use Lemma 7. More specifically, since $n^{\frac{2}{s(r-1)}} > (\log n)^3$ for large enough n, we can use Lemma 7 to conclude that the adversary can reconstruct the association graph with arbitrarily small error probability.

Second step: Identifying Group 1 among all of the groups: Now, assume the size of Group 1 is s. Without loss of generality, suppose the members of Group 1 are users $\{1, 2, \cdots, s\}$. Note that there are at most $\frac{n}{s}$ isolated groups of size s in the association graph. We call these Groups $1, 2, \cdots, \frac{n}{s}$. The adversary needs to first identify Group 1 among all of these groups.

First, for all $u \in \{1, 2, \cdots, n\}$ and all $i \in \{1, 2, \cdots, r-1\}$, the adversary computes $\widetilde{p_u(i)}$ as:

$$\widetilde{p_u(i)} = \frac{|\{k : Y_u(k) = i\}|}{m} = \frac{\widehat{M}_u(i)}{m}, \tag{4.13}$$

and as a result,

$$\widetilde{p_{\Pi(u)}(i)} = \frac{|\{k : X_u(k) = i\}|}{m} = \frac{M_u(i)}{m}, \tag{4.14}$$

where $\widehat{M}_u(i) = |\{k : Y_u(k) = i\}|$ and $M_u(i) = |\{k : X_u(k) = i\}|$. Let $\mathbf{p}_u$ be the collection of $p_u(i)$ and $\widetilde{\mathbf{p}_{\Pi(u)}}$ be the collection of $\widetilde{p_{\Pi(u)}(i)}$ for all $i \in \{1, 2, \cdots, r-1\}$:

$$\widetilde{\mathbf{p}_u} = \begin{bmatrix} \widetilde{p_u(1)} \\ \widetilde{p_u(2)} \\ \vdots \\ \widetilde{p_u(r-1)} \end{bmatrix}, \quad \widetilde{\mathbf{p}_{\Pi(u)}} = \begin{bmatrix} \widetilde{p_{\Pi(u)}(1)} \\ \widetilde{p_{\Pi(u)}(2)} \\ \vdots \\ \widetilde{p_{\Pi(u)}(r-1)} \end{bmatrix}.$$

Now, define Σ_s as the set of all permutations on s elements; for $\sigma \in \Sigma_s$, $\sigma : \{1, 2, \cdots, s\} \to \{1, 2, \cdots, s\}$ is a one-to-one mapping.

First, we provide the definition of a distance measure $D(\mathbf{\Phi}, \mathbf{\Psi})$ for vectors

$$\mathbf{\Phi} = [\mathbf{\Phi}_1 \ \ \mathbf{\Phi}_2 \ \ \cdots \ \ \mathbf{\Phi}_s],$$

$$\mathbf{\Psi} = [\mathbf{\Psi}_1 \ \ \mathbf{\Psi}_2 \ \ \cdots \ \ \mathbf{\Psi}_s],$$

where $\mathbf{\Phi}_u \in \mathbb{R}^{r-1}$ and $\mathbf{\Psi}_u \in \mathbb{R}^{r-1}$. Define

$$D(\mathbf{\Phi}, \mathbf{\Psi}) = \min_{\sigma \in \Sigma_s} \left\{ \max \left\{ ||\mathbf{\Phi}_1 - \mathbf{\Psi}_{\sigma(1)}||_\infty, ||\mathbf{\Phi}_2 - \mathbf{\Psi}_{\sigma(2)}||_\infty, \cdots, ||\mathbf{\Phi}_s - \mathbf{\Psi}_{\sigma(s)}||_\infty \right\} \right\},$$

where for all $u \in \{1, 2, \cdots, s\}$,

$$||\mathbf{\Phi}_u - \mathbf{\Psi}_{\sigma(u)}||_\infty = \max \left\{ |\Phi_u(i) - \Psi_{\sigma(u)}(i)| : i = 1, 2, \cdots, r-1 \right\}.$$

Here, let $\mathbf{P}^{(l)}$ be a vector which contains probability distributions of users belonging to Group l, and $\widetilde{\mathbf{P}^{(l)}_{\Pi}}$ be a vector which contains the estimate of the adversary about the probability distribution of users belong to Group l. For example, for Group 1, we have

$$\mathbf{P}^{(1)} = \begin{bmatrix}\mathbf{p}_1 & \mathbf{p}_2 & \cdots & \mathbf{p}_s\end{bmatrix},$$

and

$$\widetilde{\mathbf{P}^{(1)}_{\Pi}} = \begin{bmatrix}\widetilde{\mathbf{p}_{\Pi(1)}} & \widetilde{\mathbf{p}_{\Pi(2)}} & \cdots & \widetilde{\mathbf{p}_{\Pi(s)}}\end{bmatrix}.$$

Now, we claim for $m = cn^{\frac{2}{s(r-1)}+\alpha}$ and large enough n,

- $\mathbb{P}\left(D\left(\mathbf{P}^{(1)}, \widetilde{\mathbf{P}^{(1)}_{\Pi}}\right) \leq \Delta_n\right) \to 1,$
- $\mathbb{P}\left(\bigcup_{l=2}^{\frac{n}{s}}\left\{D\left(\mathbf{P}^{(1)}, \widetilde{\mathbf{P}^{(l)}_{\Pi}}\right) \leq \Delta_n\right\}\right) \to 0\,,$

where $\Delta_n = n^{-\frac{1}{s(r-1)}-\frac{\alpha}{4}}$.

Define the hypercubes of $\mathcal{F}^{(n)}$ and $\mathcal{H}^{(n)}$ as

$$\mathcal{F}^{(n)} = \left\{(\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_s) \in \left(\mathbb{R}^{(r-1)}\right)^s : \max_u\{|\mathbf{x}_u - \mathbf{p}_u|\} \leq \Delta_n, u = 1, 2, \cdots, s\right\},$$

$$\mathcal{H}^{(n)} = \left\{(\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_s) \in \left(\mathbb{R}^{(r-1)}\right)^s : \max_u\{|\mathbf{x}_u - \mathbf{p}_u|\} \leq 2\Delta_n, u = 1, 2, \cdots, s\right\},$$

Figure 4.4 shows sets $\mathcal{F}^{(n)}$ and $\mathcal{H}^{(n)}$ in the case $r = s = 2$.

First, we prove $\widetilde{\mathbf{P}^{(1)}_{\Pi}}$ is in set $\mathcal{F}^{(n)}$, thus, $D\left(\mathbf{P}^{(1)}, \widetilde{\mathbf{P}^{(1)}_{\Pi}}\right) \leq \Delta_n$. Note that for all $u \in \{1, 2, \cdots, n\}$ and all $i \in \{1, 2, \cdots, r-1\}$, a Chernoff bound yields

$$\begin{aligned}\mathbb{P}\left(\left|\frac{M_u(i)}{m} - p_u(i)\right| \geq \Delta_n\right) &\leq 2e^{-\frac{m\Delta_n^2}{3p_u}} \\ &= 2e^{-\left(cn^{\frac{2}{s(r-1)}+\alpha}\right)\left(\frac{1}{n^{\frac{1}{s(r-1)}+\frac{\alpha}{4}}}\right)^2\left(\frac{1}{3p_u}\right)} \\ &\leq 2e^{-\frac{c}{3}n^{\frac{\alpha}{2}}}. \end{aligned} \tag{4.15}$$

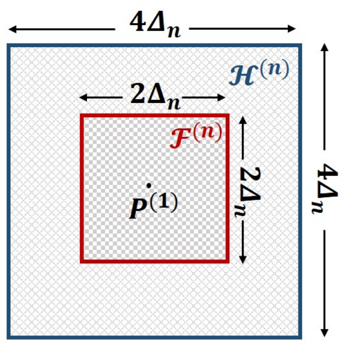


Figure 4.4: $\mathbf{P}^{(1)}$, sets $\mathcal{F}^{(n)}$ and $\mathcal{H}^{(n)}$ for the case $r = s = 2$.

Thus, for all $u \in$ Group 1 and all $i \in \{1, 2, \cdots, r-1\}$, (4.15) and the union bound yield

$$\mathbb{P}\left(D\left(\mathbf{P}^{(1)}, \widetilde{\mathbf{P}^{(1)}_{\Pi}}\right) \geq \Delta_n\right) \leq \sum_{u=1}^{s} \sum_{i=1}^{r-1} \mathbb{P}\left(\left|\frac{M_u(i)}{m} - p_u(i)\right| \geq \Delta_n\right)$$
$$\leq 2s(r-1)e^{-\frac{c}{3}n^{\frac{\alpha}{2}}} \longrightarrow 0,$$

as $n \longrightarrow \infty$. As a result, $D\left(\mathbf{P}^{(1)}, \widetilde{\mathbf{P}^{(1)}_{\Pi}}\right) \leq \Delta_n$ with high probability.

In the next step, we prove $\mathbb{P}\left(\bigcup\limits_{l=2}^{\frac{n}{s}} \left\{D\left(\mathbf{P}^{(1)}, \widetilde{\mathbf{P}^{(l)}_{\Pi}}\right) \leq \Delta_n\right\}\right) \longrightarrow 0$. Note that for all groups other than Group 1, we have

$$(4\Delta_n)^{s(r-1)}\delta_1 \leq \mathbb{P}\left(\mathbf{P}^{(l)} \in \mathcal{H}^{(n)}\right) \leq (4\Delta_n)^{s(r-1)}\delta_2,$$

and as a result,

$$\mathbb{P}\left(\mathbf{P}^{(l)} \in \mathcal{H}^{(n)}\right) \leq \delta_2(4\Delta_n)^{s(r-1)}$$
$$= \delta_2 4^{s(r-1)} \frac{1}{n^{1+\frac{\alpha}{4}s(r-1)}}.$$

Similarly, for any $\sigma \in \Sigma_s$,

$$\mathbb{P}\left(\mathbf{P}^{(l)}_{\sigma} \in \mathcal{H}^{(n)}\right) \leq \delta_2(4\Delta_n)^{s(r-1)}$$

$$= \delta_2 4^{s(r-1)} \frac{1}{n^{1+\frac{\alpha}{4}s(r-1)}},$$

and since $|\Sigma_s| = s!$, by a union bound,

$$\begin{aligned}
\mathbb{P}\left(\bigcup_{l=2}^{\frac{n}{s}} \left\{\bigcup_{\sigma \in \Sigma_s} \left\{\mathbf{P}_{\sigma}^{(l)} \in \mathcal{H}^{(n)}\right\}\right\}\right) &\leq \sum_{l=2}^{\frac{n}{s}} \sum_{\sigma \in \Sigma_s} \mathbb{P}\left(\mathbf{P}_{\sigma}^{(l)} \in \mathcal{H}^{(n)}\right) \\
&\leq \frac{n}{s} s! \delta_2 4^{s(r-1)} \frac{1}{n^{1+\frac{\alpha}{4}s(r-1)}} \\
&= (s-1)! 4^{s(r-1)} \delta_2 n^{-\frac{\alpha}{4}s(r-1)} \to 0,
\end{aligned}$$

as $n \to \infty$. Thus, all $\mathbf{P}^{(l)}$'s are outside of $\mathcal{H}^{(n)}$ with high probability.

Now, given the fact that all $\mathbf{P}^{(l)}$'s are outside of $\mathcal{H}^{(n)}$, we prove $\mathbb{P}\left(\bigcup_{l=2}^{\frac{n}{s}} \left\{D\left(\mathbf{P}^{(1)}, \widetilde{\mathbf{P}_{\Pi}^{(l)}}\right) \leq \Delta_n\right\}\right) \to 0$. We show that $\widetilde{\mathbf{P}_{\Pi}^{(l)}}$'s are close to $\mathbf{P}^{(l)}$'s, and as a result, they will be outside of $\mathcal{F}^{(n)}$. For all $u \in$ Group l and all $i \in \{1, 2, \cdots, r-1\}$, (4.15) and the union bound yield,

$$\begin{aligned}
\mathbb{P}\left(D\left(\mathbf{P}^{(1)}, \widetilde{\mathbf{P}_{\Pi}^{(l)}}\right) \leq \Delta_n\right) &= \mathbb{P}\left(D\left(\mathbf{P}^{(l)}, \widetilde{\mathbf{P}_{\Pi}^{(l)}}\right) \geq \Delta_n\right) \\
&\leq \sum_{u=1}^{s} \sum_{i=1}^{r-1} \mathbb{P}\left(\left|\frac{M_u(i)}{m} - p_u(i)\right| \geq \Delta_n\right) \\
&\leq 2s(r-1) e^{-\frac{c}{3} n^{\frac{\alpha}{2}}}.
\end{aligned}$$

Now by using a union bound, again, we have

$$\begin{aligned}
\mathbb{P}\left(\bigcup_{l=2}^{\frac{n}{s}} \left\{D\left(\mathbf{P}^{(l)}, \widetilde{\mathbf{P}_{\Pi}^{(l)}}\right) \geq \Delta_n\right\}\right) &\leq \sum_{l=2}^{\frac{n}{s}} \mathbb{P}\left(D\left(\mathbf{P}^{(l)}, \widetilde{\mathbf{P}_{\Pi}^{(l)}}\right) \geq \Delta_n\right) \\
&\leq \frac{n}{s} 2s(r-1) e^{-\frac{c}{3} n^{\frac{\alpha}{2}}} \\
&= 2n(r-1) e^{-\frac{c}{3} n^{\frac{\alpha}{2}}} \to 0,
\end{aligned}$$

as $n \to \infty$. Thus, for all $l \in \{2, 3, \cdots, \frac{n}{s}\}$, $\widetilde{\mathbf{P}_{\Pi}^{(l)}}$'s are close to $\mathbf{P}^{(l)}$'s, thus, they will be outside of $\mathcal{F}^{(n)}$ with high probability. Now, we can conclude as $n \to \infty$,

$$\mathbb{P}\left(\bigcup_{l=2}^{\frac{n}{s}} \left\{D\left(\mathbf{P}^{(1)}, \widetilde{\mathbf{P}_{\Pi}^{(l)}}\right) \leq \Delta_n\right\}\right) \to 0.$$

This means that with high probability all $\widetilde{\mathbf{P}_{\Pi}^{(l)}}$'s are outside of $\mathcal{F}^{(n)}$, so the adversary can successfully identify Group 1.

Third step: Identifying user 1 among all of the members of Group 1: In this step, we prove that, after identifying Group 1, the adversary can correctly identify each member. This step can be done using a similar approach to the one above. We define two sets $\mathcal{B}^{(n)}$ and $C^{(n)}$ around $\mathbf{p}_1$. We will show that with high probability, the true estimated value of $\mathbf{p}_1$ (shown as $\widetilde{\mathbf{p}_1}$) is inside of $\mathcal{B}^{(n)}$. Also, all $\mathbf{p}_u$'s of other members of Group 1 are outside of $C^{(n)}$, and since their estimated values are close to $\mathbf{p}_u$'s, the estimated values will be outside of $\mathcal{B}^{(n)}$. Therefore, the adversary can successfully invert the permutation Π within Group 1 and identify all of the members. Below are the details.

From (4.13) and (4.14), for all $u \in \{1, 2, \cdots, s\}$ and all $i \in \{1, 2, \cdots, r-1\}$, we have

$$\widetilde{p_u(i)} = \frac{|\{k : Y_u(k) = i\}|}{m},$$

and as a result,

$$\widetilde{p_{\Pi(u)}(i)} = \frac{|\{k : X_u(k) = i\}|}{m} = \frac{M_u(i)}{m},$$

where $M_u(i) = |\{k : X_u(k) = i\}|$. Let us define sets $\mathcal{B}^{(n)}$ and $C^{(n)}$ as

$$\mathcal{B}^{(n)} = \left\{(x_1, x_2, \cdots, x_{r-1}) \in \mathcal{R}_{\mathbf{P}} : |x_i - p_1(i)| \leq \Delta_n, i = 1, 2, \cdots, r-1\right\},$$

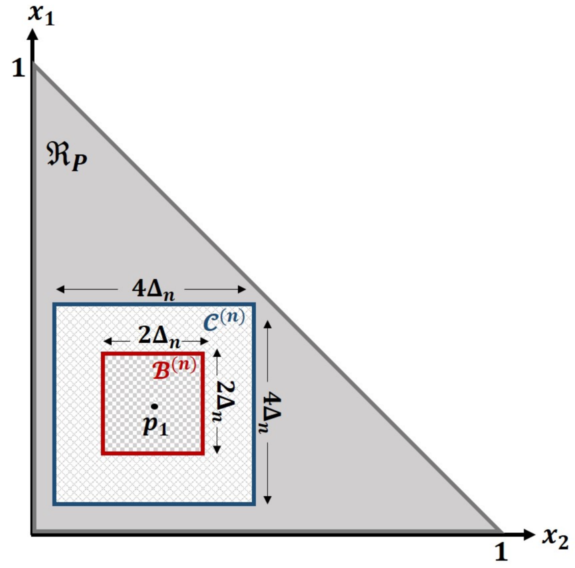


Figure 4.5: $\mathbf{p}_1$, sets $\mathcal{B}^{(n)}$ and $C^{(n)}$ in $\mathcal{R}_{\mathbf{P}}$ for case $r = 3$.

$$C^{(n)} = \left\{(x_1, x_2, \cdots, x_{r-1}) \in \mathcal{R}_{\mathbf{P}} : |x_i - p_1(i)| \leq 2\Delta_n, i = 1, 2, \cdots, r-1\right\},$$

where $\Delta_n = n^{-\frac{1}{s(r-1)}-\frac{\alpha}{4}}$. Figure 4.5 shows $\mathbf{p}_1$, sets $\mathcal{B}^{(n)}$ and $C^{(n)}$ in range of $\mathcal{R}_{\mathbf{P}}$ for case $r = 3$. Now, we claim for $m = cn^{\frac{2}{s(r-1)}+\alpha}$,

1. $\mathbb{P}\left(\widetilde{\mathbf{p}_{\Pi(1)}} \in \mathcal{B}^{(n)}\right) \to 1,$

2. $\mathbb{P}\left(\bigcup\limits_{u=2}^{s} \left\{\widetilde{\mathbf{p}_{\Pi(u)}} \in \mathcal{B}^{(n)}\right\}\right) \to 0,$

as $n \to \infty$. Thus, the adversary can identify $\Pi(1)$ by examining $\widetilde{\mathbf{p}_u}$'s and choosing the only one that belongs to $\mathcal{B}^{(n)}$.

First, we want to show that as n goes to infinity,

$$\mathbb{P}\left(\widetilde{\mathbf{p}_{\Pi(1)}} \in \mathcal{B}^{(n)}\right) \to 1.$$

For all $i \in \{1, 2, \cdots, r-1\}$, By using (4.15) and the union bound, we have

$$\mathbb{P}\left(\widetilde{\mathbf{p}_{\Pi(1)}} \notin \mathcal{B}^{(n)}\right) \leq \sum_{i=1}^{r-1} \mathbb{P}\left(\left|\frac{M_1(i)}{m} - p_1(i)\right| \geq \Delta_n\right)$$

$$\leq (r-1)\left(2e^{-\frac{c}{3}n^{\frac{\alpha}{2}}}\right),$$

thus,

$$\mathbb{P}\left(\widetilde{\mathbf{p}_{\Pi(1)}} \in \mathcal{B}^{(n)}\right) \geq 1 - 2(r-1)e^{-\frac{c}{3}n^{\frac{\alpha}{2}}} \to 1,$$

as $n \to \infty$.

Now, we need to show that as n goes to infinity,

$$\mathbb{P}\left(\bigcup_{u=2}^{s}\left\{\widetilde{\mathbf{p}_{\Pi(u)}} \in \mathcal{B}^{(n)}\right\}\right) \to 0.$$

First, we show as n goes to infinity,

$$\mathbb{P}\left(\bigcup_{u=2}^{s}\left\{\mathbf{p}_u \in C^{(n)}\right\}\right) \to 0.$$

Note

$$4\left(\Delta_n\right)^{r-1}\delta_1 < \mathbb{P}\left(\mathbf{p}_u \in C^{(n)}\right) < 4\left(\Delta_n\right)^{r-1}\delta_2,$$

and according to the union bound, for large enough n, we have

$$\begin{aligned}\mathbb{P}\left(\bigcup_{u=2}^{s}\left\{\mathbf{p}_u \in C^{(n)}\right\}\right) &\leq \sum_{u=2}^{s}\mathbb{P}\left(\mathbf{p}_u \in C^{(n)}\right)\\ &\leq 4s\left(\Delta_n\right)^{r-1}\delta_2\\ &\leq 4s\frac{1}{n^{\frac{1}{s}+\frac{\alpha(r-1)}{4}}}\delta_2 \to 0;\end{aligned}$$

thus, all $\mathbf{p}_u$'s are outside of $C^{(n)}$ with high probability.

Now, we claim that given all $\mathbf{p}_u$'s are outside of $C^{(n)}$, $\mathbb{P}\left(\widetilde{\mathbf{p}_{\Pi(u)}} \in \mathcal{B}^{(n)}\right)$ is small. Note, for all $i \in \{1, 2, \cdots, r-1\}$, by using (4.15) and the union bounds, we have

$$\begin{aligned}\mathbb{P}\left(\widetilde{\mathbf{p}_{\Pi(u)}} \in \mathcal{B}^{(n)}\right) &\leq \mathbb{P}\left(\left|\widetilde{\mathbf{p}_{\Pi(u)}} - \mathbf{p}_u\right| \geq \Delta_n\right)\\ &\leq \sum_{i=1}^{r-1} \mathbb{P}\left(\left|\frac{M_u(i)}{m} - p_u(i)\right| \geq \Delta_n\right)\\ &\leq 2(r-1)e^{-\frac{c}{3}n^{\frac{\alpha}{2}}}.\end{aligned}$$

As a result, by using another union bound, as n becomes large,

$$\mathbb{P}\left(\bigcup_{u=2}^{s}\left\{\left|\widetilde{\mathbf{p}_{\Pi(u)}} - \mathbf{p}_u\right| \geq \Delta_n\right\}\right) \leq s\left(2(r-1)e^{-\frac{c}{3}n^{\frac{\alpha}{2}}}\right) \to 0.$$

Thus, for all $u \in \{2, 3, \cdots, s\}$, $\widetilde{\mathbf{p}_{\Pi(u)}}$'s are close to $\mathbf{p}_u$'s, thus they will be outside of $\mathcal{B}^{(n)}$. Now, we can conclude as $n \to \infty$ that:

$$\mathbb{P}\left(\bigcup_{u=2}^{s}\left\{\widetilde{\mathbf{p}_{\Pi(u)}} \in \mathcal{B}^{(n)}\right\}\right) \to 0.$$

Thus, we have proved that if $m = cn^{\frac{2}{s(r-1)}+\alpha}$, there exists an algorithm for the adversary to successfully recover user 1. Remember, the adversary identifies the members of Group 1 independent of the structure of the subgraph. □

4.3.2 r-State Markov Chain Model

In Sections 4.3.1, we assumed each user's data patterns was i.i.d.; however, in this section, users' data patterns are modeled using Markov chains in which each user's data points are dependent over time. In this model, we again assume there are r possibilities for each users' data point, i.e., $X_u(k) \in \{0, 1, \cdots, r-1\}$. More specifically, each user's data set is modeled by a Markov chain with r states. It is assumed that the Markov chains of all users have the same structure but have different transition probabilities. Let E be the set of edges in the assumed transition graph, so, $(i, j) \in E$ if there exists an edge from state i to state j, meaning that $p_u(i, j) = \mathbb{P}(X_u(k+1) = j | X_u(k) = i) > 0$. The transition matrix is a square matrix used to describe the transitions of a Markov chain; thus, different users can have different transition probability matrices. Note for each state i, we have $\sum_{j=1}^{r-1} p_u(i, j) = 1$, so, the adversary can focus on a subset of size $d = |E| - r$ of the transition probabilities for recovering the entire transition matrix. Let $\mathbf{p}_u$ be the vector that contains these transition probabilities for user u. We write

$$\mathbf{p}_u = \begin{bmatrix} p_u(1) \\ \\ p_u(2) \\ \\ \vdots \\ \\ p_u(|E| - r) \end{bmatrix}, \quad \mathbf{p} = \begin{bmatrix} \mathbf{p}_1 & \mathbf{p}_2 & \cdots & \mathbf{p}_n \end{bmatrix}.$$

We also consider all $p_u(i)$'s are drawn independently from some continuous density function, $f_{\mathbf{P}}(\mathbf{p}_u)$, on the $(0, 1)^{|E|-r}$ hypercube. Define the range of distribution as

$$\mathcal{R}_{\mathbf{P}} = \left\{ (x_1, x_2, \cdots, x_{|E|-r}) \in (0, 1)^{|E|-r} : x_i > 0, x_1 + x_2 + \cdots + x_{|E|-r} < 1 \right\},$$

and as before, we assume there are $\delta_1, \delta_2 > 0$, such that

$$\begin{cases} \delta_1 \le f_{\mathbf{P}}(\mathbf{p}_u) \le \delta_2, & \mathbf{p}_u \in \mathcal{R}_{\mathbf{p}}. \\ f_{\mathbf{P}}(\mathbf{p}_u) = 0, & \mathbf{p}_u \notin \mathcal{R}_{\mathbf{p}}. \end{cases}$$

Now, we can repeat the similar steps as the previous sections to prove the following theorem.

Theorem 8. For an irreducible, aperiodic Markov chain model, if $\mathbf{Y}$ is the anonymized version of $\mathbf{X}$ as defined above, the size of the group including user 1 is s, and

- $m = \Omega\left(n^{\frac{2}{s(|E|-r)}+\alpha}\right)$, for any $\alpha > 0$;

then, user 1 has no privacy at time k.

Proof. The basic ideas behind the proof of Theorem 8 are similar to the ones for Theorems 7; thus, in this part we just focus on the differences and key ideas.

Define the random variable $M_u(i)$ as the total number of visits by user u to state i, for all $u \in \{1, 2, \cdots, n\}$ and $i \in \{0, 1, \cdots, r-1\}$. Since the Markov chain is irreducible and aperiodic, and $m \to \infty$, all $\frac{M_i(u)}{m}$ converge to their stationary values [59]. Given $M_u(i) = m_u(i)$, the transitions from state i to state j for user u has a multinomial distribution with probabilities $p_u(i, j)$. Now, considering the fact that the vector $\mathbf{p}_u$ uniquely determines the user u, the adversary can invert the anonymization permutation function in a similar way to the i.i.d. case by focusing on $\mathbf{p}_u$'s. Let

$$\mathbf{\Phi} = [\mathbf{\Phi}_1 \;\; \mathbf{\Phi}_2 \;\; \cdots \;\; \mathbf{\Phi}_s],$$

$$\mathbf{\Psi} = [\mathbf{\Psi}_1 \;\; \mathbf{\Psi}_2 \;\; \cdots \;\; \mathbf{\Psi}_s],$$

where $\mathbf{\Phi}_u \in \mathbb{R}^{|E|-r}$ and $\mathbf{\Psi}_u \in \mathbb{R}^{|E|-r}$. Define

$$D\left(\mathbf{\Phi}, \mathbf{\Psi}\right) = \min_{\sigma \in \Sigma_s} \left\{ \max\left\{ ||\mathbf{\Phi}_1 - \mathbf{\Psi}_{\sigma(1)}||_\infty, ||\mathbf{\Phi}_2 - \mathbf{\Psi}_{\sigma(2)}||_\infty, \cdots, ||\mathbf{\Phi}_s - \mathbf{\Psi}_{\sigma(s)}||_\infty \right\} \right\},$$

where for $u \in \{1, 2, \cdots, s\}$,

$$||\mathbf{\Phi}_u - \mathbf{\Psi}_{\sigma(u)}||_\infty = \max\left\{ |\Phi_u(i) - \Psi_{\sigma(u)}(i)| : i = 1, 2, \cdots, |E| - r \right\}.$$

and we claim for $m = cn^{\frac{2}{s(|E|-r)}+\alpha}$ and large enough n,

- $\mathbb{P}\left(D\left(\mathbf{P}^{(1)},\widetilde{\mathbf{P}^{(1)}_{\Pi}}\right)\leq \Delta'_n\right)\to 1,$
- $\mathbb{P}\left(\bigcup\limits_{l=2}^{\frac{n}{s}}\left\{D\left(\mathbf{P}^{(1)},\widetilde{\mathbf{P}^{(l)}_{\Pi}}\right)\leq \Delta'_n\right\}\right)\to 0\ ,$

where $\Delta'_n = n^{-\frac{1}{s(|E|-r)}-\frac{\alpha}{4}}$. This can be shown similar to the proof of Theorem 7. First, define $\mathcal{F}'^{(n)}$ and $\mathcal{H}'^{(n)}$ as

$$\mathcal{F}'^{(n)} = \left\{(\mathbf{x}_1,\mathbf{x}_2,\cdots,\mathbf{x}_s)\in\left(\mathbb{R}^{(|E|-r)}\right)^s : \max_u\{|\mathbf{x}_u-\mathbf{p}_u|\}\leq \Delta'_n, u=1,2,\cdots,s\right\}\ ;$$

$$\mathcal{H}'^{(n)} = \left\{(\mathbf{x}_1,\mathbf{x}_2,\cdots,\mathbf{x}_s)\in\left(\mathbb{R}^{(|E|-r)}\right)^s : \max_u\{|\mathbf{x}_u-\mathbf{p}_u|\}\leq 2\Delta'_n, u=1,2,\cdots,s\right\}\ ;$$

then, prove that the adversary can identify Group 1 successfully.

In the next step, the adversary has to identify each member of Group 1 correctly. Define sets $\mathcal{B}'^{(n)}$ and $C'^{(n)}$ as

$$\mathcal{B}'^{(n)} =\left\{(x_1,x_2,\cdots,x_d)\in\mathcal{R}_{\mathbf{P}} : |x_i-p_1(i)|\leq\Delta'_n, i=1,2,\cdots,d\right\},$$

$$C'^{(n)} =\left\{(x_1,x_2,\cdots,x_d)\in\mathcal{R}_{\mathbf{P}} : |x_i-p_1(i)|\leq 2\Delta'_n, i=1,2,\cdots,d\right\},$$

where $\Delta'_n = n^{-\frac{1}{s(|E|-r)}-\frac{\alpha}{4}}$. Now, we claim for $m = cn^{\frac{2}{s(|E|-r)}+\alpha}$,

1. $\mathbb{P}\left(\widetilde{\mathbf{p}_{\Pi(1)}}\in\mathcal{B}'^{(n)}\right)\to 1,$
2. $\mathbb{P}\left(\bigcup\limits_{u=2}^{s}\left\{\widetilde{\mathbf{p}_{\Pi(u)}}\in\mathcal{B}'^{(n)}\right\}\right)\to 0,$

as $n\to\infty$. This can be shown similar to the proof of Theorem 7, so the adversary can successfully recover data traces of user 1. □

Discussion 5: Note that the i.i.d. case can also be written as a Markov chain with a transition matrix with identical rows; then, $|E| = r^2$. However, for the i.i.d. case, if the adversary knows $r-1$ elements of a row, they know that row and all of the others. In other words, if we restrict the users' data models to i.i.d., then we are using a different model where $p_u(i)$'s are restricted in a way to create an i.i.d. sequence. This is a different model and is not compatible to our model for the Markov chain where $p_u(i)$'s are drawn independently from some continuous density function, $f_{\mathbf{P}}(\mathbf{p}_u)$, on the $(0,1)^{|E|-r}$ hypercube. Thus, the results of Theorem 2 cannot be applied to the i.i.d. case.

4.4 Impact of Dependency on Privacy using Anonymization and Obfuscation

Here, we consider the case when both anonymization and obfuscation techniques are employed, as shown in Figure 4.1. We assume similar obfuscation to Chapter 2. To obfuscate the users' data points, for each user u, we independently generate a random variable R_u that is uniformly distributed between 0 and a_n, where $a_n \in (0,1]$. The value of R_u shows the probability that the user's data point is changed to a different value by obfuscation, and a_n is termed the "noise level' of the system. Let $\mathbf{Z}_u$ be the vector that contains the obfuscated version of user u's data points, and $\mathbf{Z}$ be the collection of $\mathbf{Z}_u$ for all users,

$$\mathbf{Z}_u = \begin{bmatrix} Z_u(1) \\ Z_u(2) \\ \vdots \\ Z_u(m) \end{bmatrix}, \quad \mathbf{Z} = [\mathbf{Z}_1 \ \mathbf{Z}_2 \ \cdots \ \mathbf{Z}_n].$$

Thus, the adversary's observation $\mathbf{Y}$ is the anonymized version of $\mathbf{Z}$;

$$\begin{aligned}\mathbf{Y} &= \text{Perm}\left(\mathbf{Z}_1, \mathbf{Z}_2, \cdots, \mathbf{Z}_n; \Pi\right) \\ &= \left[\mathbf{Z}_{\Pi^{-1}(1)} \ \ \mathbf{X}_{\Pi^{-1}(2)} \ \ \cdots \ \ \mathbf{Z}_{\Pi^{-1}(n)}\right] \\ &= \left[\mathbf{Y}_1 \ \ \mathbf{Y}_2 \ \ \cdots \ \ \mathbf{Y}_n\right].\end{aligned}$$

4.4.1 r-State i.i.d. Model

Now, assume users' data points can have r possibilities $(0, 1, \cdots, r-1)$. Similar to Section 4.3.1, we assume $\mathbf{p}_u$'s are drawn independently from some continuous density function, $f_{\mathbf{P}}(\mathbf{p}_u)$, which has support on a subset of the $(0,1)^{r-1}$ hypercube, and $\mathbf{p}_u$, $f_{\mathbf{P}}(\mathbf{p}_u)$, and $\mathcal{R}_{\mathbf{P}}$ are defined as in Section 4.3.1.

To create a noisy version of data samples, for each user u, we independently generate a random variable R_u that is uniformly distributed between 0 and a_n, where $a_n \in (0,1]$[2]. Then, the obfuscated data is obtained by passing the users' data through an r-ary symmetric channel with a random error probability R_u, so for $j \in \{0, 1, \cdots, r-1\}$:

$$\mathbb{P}(Z_u(k) = j | X_u(k) = i) = \begin{cases} 1 - R_u, & \text{for } j = i. \\ \frac{R_u}{r-1}, & \text{for } j \neq i. \end{cases}$$

The effect of the obfuscation is to alter the probability distribution function of each user's data points in a way that is unknown to the adversary, since it is independent of all past activity of the user, and hence, the obfuscation inhibits user identification. For each user, R_u is generated once and is kept constant for the collection of data points of length m, thus providing a very low-weight obfuscation algorithm.

[2] It is desirable that our results are true over the largest set of strategies that users can employ. In fact, our results would apply to a general set of distributions and are true for any random noise with support that extends out to the maximum amount of a_n. The reason that we have used a uniformly random noise is that we want to have a similar mechanism as Chapter 2 to have a good comparison between the results of this chapter and Chapter 2 to show that dependency is a significant detriment to the privacy of users.

Now, define

$$Q_u(i) = \mathbb{P}\left(Z_u(k) = i\right),$$

where

$$\begin{aligned} Q_u(i) &= P_u(i)(1 - R_u) + (1 - P_u(i))R_u \\ &= P_u(i) + (1 - 2P_u(i))R_u. \end{aligned} \tag{4.16}$$

The vectors $\mathbf{Q}_u$ and $\mathbf{Q}$ which contain the obfuscated probabilities are defined as below:

$$\mathbf{Q}_u = \begin{bmatrix} Q_u(1) \\ Q_u(2) \\ \vdots \\ Q_u(r-1) \end{bmatrix}, \quad \mathbf{Q} = \left[\mathbf{Q}_1 \ \ \mathbf{Q}_2 \ \ \cdots \ \ \mathbf{Q}_n\right],$$

and the vector containing the permutation of those probabilities after anonymization is $\mathbf{W}$. Thus,

$$\begin{aligned} \mathbf{W} &= \text{Perm}\left(\mathbf{Q}_1, \mathbf{Q}_2, \cdots, \mathbf{Q}_n; \Pi\right) \\ &= \left[\mathbf{Q}_{\Pi^{-1}(1)} \ \ \mathbf{Q}_{\Pi^{-1}(2)} \ \ \cdots \ \ \mathbf{Q}_{\Pi^{-1}(n)}\right] \\ &= \left[\mathbf{W}_1 \ \ \mathbf{W}_2 \ \ \cdots \ \ \mathbf{W}_n\right]. \end{aligned}$$

Theorem 9. For the above r-state model, if $\mathbf{Z}$ is the obfuscated version of $\mathbf{X}$, and $\mathbf{Y}$ is the anonymized version of $\mathbf{Z}$ as defined above, the size of the group including user 1 is s, and

- $m = \Omega\left(cn^{\frac{2}{s(r-1)}+\alpha}\right)$ for any $\alpha > 0$;
- $R_u \sim \text{Uniform}[0, a_n]$, where $a_n = O\left(n^{-\frac{1}{s(r-1)}-\beta}\right)$ for any $\beta > \frac{\alpha}{4}$;

then, user 1 has no privacy at time k.

Discussion 6: It is insightful to compare this result to Theorem 2 of 2. We can see that when users' traces are dependent, the required level of obfuscation and anonymization to achieve privacy is significantly higher. Therefore, we see that dependency can significantly reduce the privacy of users. However, note that the asymptotic noise level is still zero in this case. Specifically, if $A_m(u) = \frac{|\{k: Z_u(k) \neq X_u(k)\}|}{m}$, then

$$\mathbb{E}[A_m(u)] = \mathbb{E}[A_m] = O\left(n^{-\frac{1}{s(r-1)}-\beta}\right) \to 0,$$

implying that the asymptotic noise level is zero.

Proof of Theorem 9:

Proof. The proof of Theorem 9 is similar to the proof of Theorem 7 and consists of three parts:

- **First step:** Showing the adversary can reconstruct the association graph of the obfuscated and anonymized version of data with an arbitrarily small error probability.
- **Second step:** Showing the adversary can uniquely identify Group 1 with an arbitrarily small error probability.
- **Third step:** Showing the adversary can successfully identify all of the members of Group 1 with an arbitrarily small error probability.

First step: Reconstruction of the association graph: In Lemma 7, we show that for the case of anonymization, the adversary can reconstruct the entire association graph of the anonymized data with an arbitrarily small error probability if the number of the adversary's observations per user (m) is bigger than $(\log n)^3$. Since obfuscation is done independently (from other users' obfuscation and from users' data), it does not change the association graph. Therefore, since $n^{\frac{2}{s(r-1)}} > (\log n)^3$, we can use Lemma 7 to show the adversary can reconstruct the association graph of the obfuscated and anonymized data with an arbitrarily small error probability.

Second step: Identifying Group 1 among all of the groups: Now, assume the size of Group 1 is s. Without loss of generality, suppose the members of Group 1 are users $\{1, 2, \cdots, s\}$, so there are at most $\frac{n}{s}$ groups of size s. We call these Groups $1, 2, \cdots, \frac{n}{s}$. The adversary needs to first identify the Group 1 among all of these groups.

According to Section 4.3.1, Σ_s is defined as the set of all permutation on s elements, and $\mathbf{P}^{(l)}$ is a vector which contains probability distributions of users belong to Group l, and $\widetilde{\mathbf{P}^{(l)}_{\Pi}}$ is a vector which contains the estimate of adversary about the probability distribution of users belong to Group l. For example, For Group 1, we have

$$\mathbf{P}^{(1)} = \left[\mathbf{p}_1 \ \mathbf{p}_2 \ \cdots \ \mathbf{p}_s\right],$$

and

$$\widetilde{\mathbf{P}^{(1)}_{\Pi}} = \left[\widetilde{\mathbf{p}_{\Pi(1)}} \ \widetilde{\mathbf{p}_{\Pi(2)}} \ \cdots \ \widetilde{\mathbf{p}_{\Pi(s)}}\right].$$

We claim for $m = cn^{\frac{2}{s(r-1)}+\alpha}$, $a_n = c'n^{-\left(\frac{1}{s(r-1)}+\beta\right)}$, and large enough n,

- $\mathbb{P}\left(D\left(\mathbf{P}^{(1)}, \widetilde{\mathbf{P}^{(1)}_{\Pi}}\right) \le \Delta_n\right) \to 1,$
- $\mathbb{P}\left(\bigcup_{l=2}^{\frac{n}{s}} \left\{D\left(\mathbf{P}^{(1)}, \widetilde{\mathbf{P}^{(l)}_{\Pi}}\right) \le \Delta_n\right\}\right) \to 0,$

where $\Delta_n = n^{-\frac{1}{s(r-1)}-\frac{\alpha}{4}}$. As in Section 4.3.1,

$$\mathcal{F}^{(n)} = \left\{(\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_s) \in \left(\mathbb{R}^{(r-1)}\right)^s : \max_u\{|\mathbf{x}_u - \mathbf{p}_u|\} \le \Delta_n, u = 1, 2, \cdots, s\right\},$$

$$\mathcal{H}^{(n)} = \left\{(\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_s) \in \left(\mathbb{R}^{(r-1)}\right)^s : \max_u\{|\mathbf{x}_u - \mathbf{p}_u|\} \leq 2\Delta_n, u = 1, 2, \cdots, s\right\}.$$

First, we prove, as $n \to \infty$,

$$\mathbb{P}\left(D\left(\mathbf{P}^{(1)}, \widetilde{\mathbf{P}^{(1)}_{\Pi}}\right) \leq \Delta_n\right) \to 1.$$

Note that for all $u \in \{1, 2, \cdots, n\}$ and all $i \in \{1, 2, \cdots, r-1\}$, the adversary computes $\widetilde{p_u(i)}$ as follow:

$$\widetilde{p_u(i)} = \frac{|\{k : Y_u(k) = i\}|}{m}, \tag{4.17}$$

and as a result,

$$\widetilde{p_{\Pi(u)}(i)} = \frac{|\{k : Z_u(k) = i\}|}{m} = \frac{\breve{M}_u(i)}{m}, \tag{4.18}$$

where $\breve{M}_u(i) = |\{k : Z_u(k) = i\}|$. Now, for all $u \in \{1, 2, \cdots, n\}$ and all $i \in \{0, 1, \cdots, r-1\}$, we have

$$\begin{aligned}\mathbb{P}\left(\left|\frac{\breve{M}_u(i)}{m} - p_u(i)\right| \leq \Delta_n\right) &= \mathbb{P}\left(p_u(i) - \Delta_n \leq \frac{\breve{M}_u(i)}{m} \leq p_u(i) + \Delta_n\right) \\ &= \mathbb{P}\left(p_u(i) - \Delta_n - q_u(i) \leq \frac{\breve{M}_u(i)}{m} - q_u(i) \leq p_u(i) + \Delta_n - q_u(i)\right).\end{aligned}$$

Note that for all $u \in \{1, 2, \cdots, n\}$ and all $i \in \{0, 1, \cdots, r-1\}$, we have

$$\begin{aligned}|p_u(i) - q_u(i)| &= |1 - 2p_u(i)|R_u \\ &\leq R_u \leq a_n,\end{aligned}$$

so, we can conclude for all $u \in \{1, 2, \cdots, n\}$ and all $i \in \{0, 1, \cdots, r-1\}$,

$$\begin{aligned}
\mathbb{P}\left(\left|\frac{\breve{M}_u(i)}{m} - p_u(i)\right| \le \Delta_n\right) &= \mathbb{P}\left(p_u(i) - \Delta_n - q_u(i) \le \frac{\breve{M}_u(i)}{m} - q_u(i) \le p_u(i) + \Delta_n - q_u(i)\right) \\
&\ge \mathbb{P}\left(-\Delta_n + a_n \le \frac{\breve{M}_u(i)}{m} - q_u(i) \le -a_n + \Delta_n\right) \\
&= \mathbb{P}\left(\left|\frac{\breve{M}_u(i)}{m} - q_u(i)\right| \le m(\Delta_n - a_n)\right). \qquad (4.19)
\end{aligned}$$

By employing a Chernoff bound, we have

$$\begin{aligned}
\mathbb{P}\left(\left|\frac{\breve{M}_u(i)}{m} - q_u(i)\right| \le m(\Delta_n - a_n)\right) &\ge 1 - 2e^{-\frac{(\Delta_n - a_n)^2}{3q_u(i)}} \\
&\ge 1 - 2e^{-\left(\frac{1}{3q_u(i)}\right)\left(cn^{\frac{2}{s(r-1)}+\alpha}\right)\left(\frac{1}{n^{\frac{1}{s(r-1)}+\frac{\alpha}{4}}} - \frac{c'}{n^{\frac{1}{s(r-1)}+\beta}}\right)^2} \\
&\ge 1 - 2e^{-\frac{1}{3}\left(cn^{\frac{2}{s(r-1)}+\alpha}\right)\left(\frac{1}{n^{\frac{1}{s(r-1)}+\frac{\alpha}{4}}} - \frac{c'}{n^{\frac{1}{s(r-1)}+\beta}}\right)^2} \qquad (4.20)
\end{aligned}$$

Now from (4.19) and (4.20), we can conclude for all $u \in \{1, 2, \cdots, n\}$ and all $i \in \{0, 1, \cdots, r-1\}$,

$$\mathbb{P}\left(\left|\frac{\breve{M}_u(i)}{m} - p_u(i)\right| \le \Delta_n\right) \ge 1 - 2e^{-\frac{1}{3}\left(cn^{\frac{2}{s(r-1)}+\alpha}\right)\left(\frac{1}{n^{\frac{1}{s(r-1)}+\frac{\alpha}{4}}} - \frac{c'}{n^{\frac{1}{s(r-1)}+\beta}}\right)^2},$$

and

$$\mathbb{P}\left(\left|\frac{\breve{M}_u(i)}{m} - p_u(i)\right| \ge \Delta_n\right) \le 2e^{-\frac{1}{3}\left(cn^{\frac{2}{s(r-1)}+\alpha}\right)\left(\frac{1}{n^{\frac{1}{s(r-1)}+\frac{\alpha}{4}}} - \frac{c'}{n^{\frac{1}{s(r-1)}+\beta}}\right)^2}. \qquad (4.21)$$

Now, for all $u \in$ Group 1, all $i \in \{1, 2, \cdots, r-1\}$ and any $\beta > \frac{\alpha}{4}$, (4.21) and the union bound yield

$$\mathbb{P}\left(D\left(\mathbf{P}^{(1)}, \widetilde{\mathbf{P}_{\Pi}^{(1)}}\right) \ge \Delta_n\right) \le \sum_{u=1}^{s} \sum_{i=1}^{r-1} \mathbb{P}\left(\left|\frac{\breve{M}_u(i)}{m} - p_u(i)\right| \ge \Delta_n\right)$$

$$\leq 2s(r-1)e^{-\frac{1}{3}\left(cn^{\frac{2}{s(r-1)}+\alpha}\right)\left(\frac{1}{n^{\frac{1}{s(r-1)}+\frac{\alpha}{4}}}-\frac{c'}{n^{\frac{1}{s(r-1)}+\beta}}\right)^2} \to 0,$$

as $n \to \infty$. As a result,

$$\mathbb{P}\left(D\left(\mathbf{P}^{(1)}, \widetilde{\mathbf{P}_{\Pi}^{(1)}}\right) \leq \Delta_n\right) \to 1,$$

as $n \to \infty$.

In the next step, we prove $\mathbb{P}\left(\bigcup_{l=2}^{\frac{n}{s}}\left\{D\left(\mathbf{P}^{(1)}, \widetilde{\mathbf{P}_{\Pi}^{(l)}}\right) \leq \Delta_n\right\}\right) \to 0$. For all groups other than Group 1, we have

$$(4\Delta_n)^{s(r-1)}\delta_1 \leq \mathbb{P}\left(\mathbf{P}^{(l)} \in \mathcal{H}'^{(n)}\right) \leq (4\Delta_n)^{s(r-1)}\delta_2,$$

and as a result,

$$\begin{aligned}\mathbb{P}\left(\mathbf{P}^{(l)} \in \mathcal{H}^{(n)}\right) &\leq \delta_2(4\Delta_n)^{s(r-1)}\\ &= \delta_2 4^{s(r-1)}\frac{1}{n^{1+\frac{\alpha}{4}s(r-1)}}.\end{aligned}$$

Similarly, for any $\sigma \in \Sigma_s$,

$$\begin{aligned}\mathbb{P}\left(\mathbf{P}_{\sigma}^{(l)} \in \mathcal{H}'^{(n)}\right) &\leq \delta_2(4\Delta_n)^{s(r-1)}\\ &= \delta_2 4^{s(r-1)}\frac{1}{n^{1+\frac{\alpha}{4}s(r-1)}},\end{aligned}$$

and since $|\Sigma_s| = s!$, by a union bound,

$$\begin{aligned}\mathbb{P}\left(\bigcup_{l=2}^{\frac{n}{s}}\left\{\bigcup_{\sigma\in\Sigma_s}\left\{\mathbf{P}_{\sigma}^{(l)} \in \mathcal{H}^{(n)}\right\}\right\}\right) &\leq \sum_{l=2}^{\frac{n}{s}}\sum_{\sigma\in\Sigma_s}\mathbb{P}\left(\mathbf{P}_{\sigma}^{(l)} \in \mathcal{H}^{(n)}\right)\\ &\leq \frac{n}{s}s!\delta_2 4^{s(r-1)}\frac{1}{n^{1+\frac{\alpha}{4}s(r-1)}}\\ &= (s-1)!4^{s(r-1)}\delta_2 n^{-\frac{\alpha}{4}s(r-1)} \to 0,\end{aligned}$$

as $n \to \infty$. Thus, all $\mathbf{P}^{(l)}$'s are outside of $\mathcal{H}^{(n)}$ with high probability.

Now, we claim that given all $\mathbf{P}^{(l)}$'s are outside of $\mathcal{H}^{(n)}$, $\mathbb{P}\left(\bigcup_{l=2}^{\frac{n}{s}}\left\{D\left(\mathbf{P}^{(1)}, \widetilde{\mathbf{P}_{\Pi}^{(l)}}\right) \leq \Delta_n\right\}\right)$ is arbitrarily small. In other words, by using a Chernoff bound, it is shown $\widetilde{\mathbf{P}^{(l)}}$'s are close to $\mathbf{P}^{(l)}$'s, and they will be outside of $\mathcal{F}^{(n)}$. Thus, for all $u \in$ Group l and all $i \in \{1, 2, \cdots, r-1\}$, (4.21) and the union bound yield

$$\begin{aligned}
\mathbb{P}\left(D\left(\mathbf{P}^{(1)}, \widetilde{\mathbf{P}_{\Pi}^{(l)}}\right) \leq \Delta_n\right) &= \mathbb{P}\left(D\left(\mathbf{P}^{(l)}, \widetilde{\mathbf{P}_{\Pi}^{(l)}}\right) \geq \Delta_n\right) \\
&\leq \sum_{u=1}^{s}\sum_{i=1}^{r-1} \mathbb{P}\left(\left|\frac{\breve{M}_u(i)}{m} - p_u(i))\right| \leq \Delta_n\right) \\
&\leq 2s(r-1)e^{-\frac{1}{3}\left(cn^{\frac{2}{s(r-1)}+\alpha}\right)\left(\frac{1}{n^{\frac{1}{s(r-1)}+\frac{\alpha}{4}}}-\frac{c'}{n^{\frac{1}{s(r-1)}+\beta}}\right)^2}.
\end{aligned}$$

Now, by using a union bound again, we can conclude, for any $\beta > \frac{\alpha}{4}$,

$$\begin{aligned}
\mathbb{P}\left(\bigcup_{l=2}^{\frac{n}{s}}\left\{D\left(\mathbf{P}^{(l)}, \widetilde{\mathbf{P}_{\Pi}^{(l)}}\right) \leq \Delta_n\right\}\right) &\leq \sum_{l=2}^{\frac{n}{s}} \mathbb{P}\left(D\left(\mathbf{P}^{(l)}, \widetilde{\mathbf{P}_{\Pi}^{(l)}}\right) \leq \Delta_n\right) \\
&\leq 2n(r-1)e^{-\frac{1}{3}\left(cn^{\frac{2}{s(r-1)}+\alpha}\right)\left(\frac{1}{n^{\frac{1}{s(r-1)}+\frac{\alpha}{4}}}-\frac{c'}{n^{\frac{1}{s(r-1)}+\beta}}\right)^2} \to 0,
\end{aligned}$$

as $n \to \infty$. Thus, we have shown that for all $l \in \{1, 2, \cdots, \frac{n}{s}\}$, $\widetilde{\mathbf{P}^{(l)}}$'s are close to $\mathbf{P}^{(l)}$, which are outside of set $\mathcal{F}^{(n)}$. As a result, as $n \to \infty$,

$$\mathbb{P}\left(\bigcup_{l=2}^{\frac{n}{s}}\left\{D\left(\mathbf{P}^{(1)}, \widetilde{\mathbf{P}_{\Pi}^{(l)}}\right) \leq \Delta_n\right\}\right) \to 0.$$

Third step: Identifying user 1 **among all of the members of Group** 1**:** In this step, we need to prove that after identifying Group 1, the adversary can correctly identify each member. In other words, the adversary should identify the permutation of Group 1.

From (4.17) and (4.18), for all $u \in \{1, 2, \cdots, s\}$ and all $i \in \{1, 2, \cdots, r-1\}$, we have

$$\widetilde{p_u(i)} = \frac{|\{k : Y_u(k) = i\}|}{m},$$

and as a result,

$$\widetilde{p_{\Pi(u)}(i)} = \frac{|\{k : Z_u(k) = i\}|}{m} = \frac{\breve{M}_u(i)}{m},$$

where $\breve{M}_u(i) = |\{k : Z_u(k) = i\}|$.

As in Section 4.3.1, we define sets $\mathcal{B}^{(n)}$ and $C^{(n)}$ as

$$\mathcal{B}^{(n)} = \Big\{(x_1, x_2, \cdots, x_{r-1}) \in \mathcal{R}_{\mathbf{P}} : |x_i - p_1(i)| \leq \Delta_n', i = 1, 2, \cdots, r-1\Big\},$$

$$C^{(n)} = \Big\{(x_1, x_2, \cdots, x_{r-1}) \in \mathcal{R}_{\mathbf{P}} : |x_i - p_1(i)| \leq 2\Delta_n', i = 1, 2, \cdots, r-1\Big\},$$

where $\Delta_n = n^{-\frac{1}{s(r-1)} - \frac{\alpha}{4}}$. We claim that for $m = cn^{\frac{2}{s(r-1)} + \alpha}$ and $a_n = c'n^{-\left(\frac{1}{s(r-1)} + \beta\right)}$,

1. $\mathbb{P}\left(\widetilde{\mathbf{p}_{\Pi(1)}} \in \mathcal{B}^{(n)}\right) \to 1,$
2. $\mathbb{P}\left(\bigcup\limits_{u=2}^{s} \left\{\widetilde{\mathbf{p}_{\Pi(u)}} \in \mathcal{B}^{(n)}\right\}\right) \to 0,$

as $n \to \infty$. Thus, the adversary can identify $\Pi(1)$ by examining $\widetilde{\mathbf{p}_u}$'s and choosing the only one that belongs to $\mathcal{B}^{(n)}$.

First, we show that as n goes to infinity,

$$\mathbb{P}\left(\widetilde{\mathbf{p}_{\Pi(1)}} \in \mathcal{B}^{(n)}\right) \to 1.$$

According to (4.21) and the union bound, for all $u \in$ Group 1 and all $i \in \{1, 2, \cdots, r-1\}$, we have

$$\begin{aligned}\mathbb{P}\left(\widetilde{\mathbf{p}_{\Pi(1)}} \notin \mathcal{B}^{(n)}\right) &\le \sum_{i=1}^{r-1} \mathbb{P}\left(\left|\frac{\breve{M}_1(i)}{m} - p_1(i)\right| \ge \Delta_n\right) \\ &\le (r-1)\left(2e^{-\frac{1}{3}\left(cn^{\frac{2}{s(r-1)}+\alpha}\right)\left(\frac{1}{n^{\frac{1}{s(r-1)}+\frac{\alpha}{4}}}-\frac{c'}{n^{\frac{1}{s(r-1)}+\beta}}\right)^2}\right),\end{aligned}$$

thus,

$$\mathbb{P}\left(\widetilde{\mathbf{p}_{\Pi(1)}} \in \mathcal{B}^{(n)}\right) \le 1-(r-1)\left(2e^{-\frac{1}{3}\left(cn^{\frac{2}{s(r-1)}+\alpha}\right)\left(\frac{1}{n^{\frac{1}{s(r-1)}+\frac{\alpha}{4}}}-\frac{c'}{n^{\frac{1}{s(r-1)}+\beta}}\right)^2}\right) \longrightarrow 1,$$

as $n \longrightarrow \infty$.

Now, we need to show that as n goes to infinity,

$$\mathbb{P}\left(\bigcup_{u=2}^{s}\left\{\widetilde{\mathbf{p}_{\Pi(u)}} \in \mathcal{B}^{(n)}\right\}\right) \longrightarrow 0.$$

First, we show as n goes to infinity,

$$\mathbb{P}\left(\bigcup_{u=2}^{s}\left\{\mathbf{p}_u \in \mathcal{C'}^{(n)}\right\}\right) \longrightarrow 0.$$

Note for all $u \in \{2, 3, \cdots, s\}$,

$$4\left(\Delta_n\right)^{r-1}\delta_1 < \mathbb{P}\left(\mathbf{p}_u \in \mathcal{C'}^{(n)}\right) < 4\left(\Delta_n\right)^{r-1}\delta_2,$$

and according to the union bound,

$$\mathbb{P}\left(\bigcup_{u=2}^{s}\left\{\mathbf{p}_u \in \mathcal{C}^{(n)}\right\}\right) \le \sum_{u=2}^{s}\mathbb{P}\left(\mathbf{p}_u \in \mathcal{C}^{(n)}\right)$$

$$
\begin{aligned}
&\leq 4s\left(\Delta_n\right)^{r-1}\delta_2 \\
&\leq 4s\frac{1}{n^{\frac{1}{s}+\frac{\alpha(r-1)}{4}}}\delta_2 \longrightarrow 0;
\end{aligned}
$$

as $n \longrightarrow \infty$. Thus, all $\mathbf{p}_u$'s are outside of $C^{(n)}$ with high probability.

Now, we claim that given all $\mathbf{p}_u$'s are outside of $C^{(n)}$, $\mathbb{P}\left(\widetilde{\mathbf{p}_{\Pi(u)}} \in \mathcal{B}^{(n)}\right)$ is arbitrarily small. Note that for all $u \in \{2, 3, \cdots, s\}$ and all $i \in \{1, 2, \cdots, r-1\}$, (4.21) and the union bounds yield

$$
\begin{aligned}
\mathbb{P}\left(\widetilde{\mathbf{p}_{\Pi(u)}} \in \mathcal{B}^{(n)}\right) &\leq \mathbb{P}\left(\left|\widetilde{\mathbf{p}_{\Pi(u)}} - \mathbf{p}_u\right| \geq \Delta_n\right) \\
&\leq \sum_{i=1}^{r-1} \mathbb{P}\left(\left|\widetilde{p_{\Pi(u)}(i)} - p_u(i)\right| \geq \Delta_n\right) \\
&\leq 2(r-1)e^{-\frac{1}{3}\left(cn^{\frac{2}{s(r-1)}+\alpha}\right)\left(\frac{1}{n^{\frac{1}{s(r-1)}+\frac{\alpha}{4}}}-\frac{c'}{n^{\frac{1}{s(r-1)}+\beta}}\right)^2}.
\end{aligned}
$$

As a result, by using a union bound again, as n becomes large,

$$
\mathbb{P}\left(\bigcup_{u=2}^{s}\left\{\left|\widetilde{\mathbf{p}_{\Pi(u)}} - \mathbf{p}_u\right| \geq \Delta_n\right\}\right) \leq s\left(2(r-1)e^{-\frac{1}{3}\left(cn^{\frac{2}{s(r-1)}+\alpha}\right)\left(\frac{1}{n^{\frac{1}{s(r-1)}+\frac{\alpha}{4}}}-\frac{c'}{n^{\frac{1}{s(r-1)}+\beta}}\right)^2}\right) \longrightarrow 0.
$$

Thus, for all $u \in \{2, 3, \cdots, s\}$, $\widetilde{\mathbf{p}_{\Pi(u)}}$'s are close to $\mathbf{p}_u$'s, thus they will be outside of $\mathcal{B}^{(n)}$. Now, we can conclude as $n \longrightarrow \infty$ that:

$$
\mathbb{P}\left(\bigcup_{u=2}^{s}\left\{\widetilde{\mathbf{p}_{\Pi(u)}} \in \mathcal{B}^{(n)}\right\}\right) \longrightarrow 0.
$$

So the adversary can successfully recover $Z_1(k)$. Since $Z_1(k) = X_1(k)$ with probability $1 - R_u = 1 - o(1)$, the adversary can recover $X_1(k)$ with vanishing error probability. □

4.4.2 r-State Markov Chain Model

In this section, users' data patterns are modeled using Markov chains and there are r possibilities for users' data patterns. Similar to Section 4.3.2, we assume $p_u(i)$'s are drawn independently from some continuous density function, $f_{\mathbf{P}}(\mathbf{p}_u)$, on the $(0,1)^{|E|-r}$ hypercube, and $\mathbf{p}_u$, $f_{\mathbf{P}}(\mathbf{p}_u)$, and $\mathcal{R}_{\mathbf{P}}$ are defined in Section 4.3.2.

By using the general idea stated in Section 4.3.2, we can now repeat the similar reasoning as Theorem 9 to show the following theorem.

Theorem 10. For an irreducible, aperiodic Markov chain model, iff $\mathbf{Z}$ is the obfuscated version of $\mathbf{X}$, and $\mathbf{Y}$ is the anonymized version of $\mathbf{Z}$ as defined above, the size of the group including user 1 is s, and

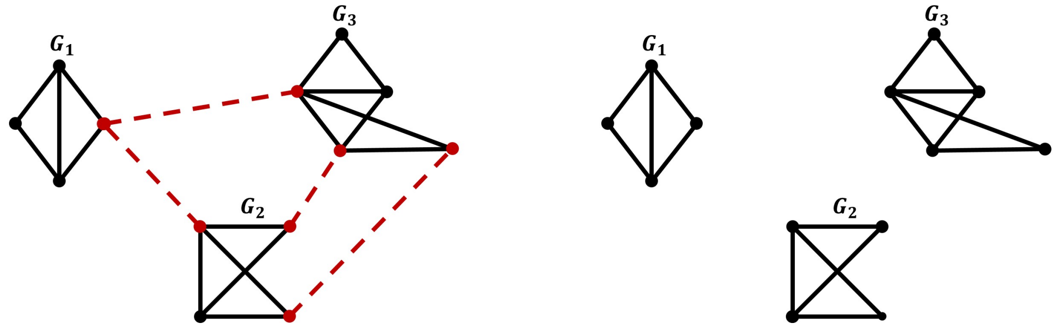
- $m = \Omega\left(n^{\frac{2}{s(|E|-r)}+\alpha}\right)$ for any $\alpha > 0$;
- $R_u \sim \text{Uniform}[0, a_n]$, where $a_n = O\left(n^{-\frac{1}{s(|E|-r)}-\beta}\right)$ for any $\beta > \frac{\alpha}{4}$;

then, user 1 has no privacy at time k.

4.5 More General Setting for the Association Graph

The association graph structure that we have studied so far was somewhat general except for one aspect: We assumed that people in a group can have dependency but they are independent from members of other groups. It is natural to assume that there could be dependency between members of each group and outside members. Here we discuss how to apply the developed results to this more general setting.

Similar to [23, 32, 35, 37, 38, 53, 75, 77, 100, 125], we consider a community structure with strong intra-community connections and weak inter-community connection. In the community structure the nodes of the network can be grouped into sets of users such that each set of users is densely connected internally as shown in Figure 4.6a. Here, we also assume that the adversary has some knowledge about all of the covariances between users



(a) A sketch of a small network displaying community structure.

(b) The association graph consists of disjoint subgraphs.

Figure 4.6: The adversary uses their prior knowledge to break inter-community edges.

in addition to the marginal probability distributions: they know whether the value of each covariance is less than or higher than a specific threshold. We show that the adversary can reliably reconstruct the entire association graph for *the anonymized version of the data* (i.e., the observed data traces) with relatively few observations.

Let $G(\mathcal{V}, F)$ denote the association graph with set of nodes $\mathcal{V}$, ($|\mathcal{V}| = n$), and set of edges F. In this case, we use an association graph based on a threshold as follows: we assume two vertices (users) are connected if their data sets are strongly correlated, and are not connected if their data sets are weakly correlated. More specifically,

- $(u, u') \notin F$ iff $\text{Cov}\left(X_u(k); X_{u'}(k)\right) \leq \epsilon_1$,
- $(u, u') \in F$ iff $\text{Cov}\left(X_u(k); X_{u'}(k)\right) \geq \epsilon_2$,

where $\text{Cov}\left(X_u(k); X_{u'}(k)\right)$ is the covariance between the k^{th} data point of user u and user u'.

Lemma 8. Consider a general association graph, $G(\mathcal{V}, F)$, based on the threshold as described above. If the adversary obtains $m = (\log n)^3$ anonymized observations per user, they can construct $\widetilde{G} = \widetilde{G}(\widetilde{\mathcal{V}}, \widetilde{F})$, where $\widetilde{\mathcal{V}} = \{\Pi(u) : u \in \mathcal{V}\} = \mathcal{V}$, such that with high probability, for all $u, u' \in \mathcal{V}$; $(u, u') \in F$ iff $(\Pi(u), \Pi(u')) \in \widetilde{F}$. We write this statement as $\mathbb{P}(\widetilde{G} \simeq G) \to 1$.

Proof. Note for $u, u' \in \{1, 2, \cdots, n\}$, we write $v = \Pi(u)$ and $v' = \Pi(u')$. We provide an algorithm for the adversary that with high probability obtains all edges of F correctly. For each pair w and w', the adversary computes $\widetilde{Cov_{vv'}}$ as follows:

$$\widetilde{Cov_{vv'}} = \frac{\sum_{i=1}^{r-1}\sum_{j=1}^{r-1} ij\widehat{M}_{vv'}(i,j)}{m} - \frac{\sum_{i=1}^{r-1} i\widehat{M}_{v}(i)}{m}\frac{\sum_{i=1}^{r-1} i\widehat{M}_{v'}(i)}{m} \tag{4.22}$$

where

$$\widehat{M}_{vv'}(i,j) = |\{k : Y_v(k) = i, Y_{v'}(k) = j\}|.$$

$$\widehat{M}_{v}(i) = |\{k : Y_v(k) = i\}|.$$

$$\widehat{M}_{v'}(j) = |\{k : Y_{v'}(k) = j\}|.$$

After observing $m = (\log n)^3$ data points per user and computing the above expressions, the adversary constructs $\widetilde{G}$ in the following way:

- If $|\widetilde{Cov_{vv'}}| \leq \epsilon_1$, then $(v, v') \notin \widetilde{F}$.
- If $|\widetilde{Cov_{vv'}}| \geq \epsilon_2$, then $(v, v') \in \widetilde{F}$.

We show the above method yields $\mathbb{P}(\widetilde{G} \simeq G) \longrightarrow 1$ as $n \longrightarrow \infty$, as follows. Note

$$\widehat{M}_{vv'}(i,j) \sim \text{Binomial}(m, w_{vv'}(i,j)),$$

$$\widehat{M}_{v}(i) \sim \text{Binomial}(m, w_{v}(i)),$$

$$M_{v'}(i) \sim \text{Binomial}(m, w_{v'}(i)),$$

where $w_{vv'}(i,j) = \mathbb{P}(Y_v(k) = i, Y_{v'}(k) = j)$, $w_v(i) = \mathbb{P}(Y_v(k) = i)$, and $w_{v'}(i) = \mathbb{P}(Y_{v'}(k) = i)$. From proof of Lemma 7, by using (4.4), for all $v, v' \in \{1, 2, \cdots, n\}$ and all $i, j \in \{0, 1, \cdots, r-1\}$, we have

$$0 \leq mw_{vv'}(i,j) - m^{\frac{3}{4}} \leq \widehat{M}_{vv'}(i,j) \leq mw_{vv'}(i,j) + m^{\frac{3}{4}}. \tag{4.23}$$

$$0 \le mw_v(i) - m^{\frac{3}{4}} \le \widehat{M}_v(i) \le mw_v(i) + m^{\frac{3}{4}}. \tag{4.24}$$

$$0 \le mw_{v'}(i) - m^{\frac{3}{4}} \le \widehat{M}_{v'}(i) \le mw_v(i) + m^{\frac{3}{4}}. \tag{4.25}$$

$A_{vv'}(i,j)$ is defined as the event that (4.23), (4.24), and (4.25) are all valid, thus, based on proof of Lemma 7, we have

$$\mathbb{P}\left(\bigcap_{v=1}^{n}\bigcap_{v'=1}^{n}\bigcap_{i=0}^{r-1}\bigcap_{j=0}^{r-1}\{A_{vv'}(i,j)\}\right) \longrightarrow 1, \tag{4.26}$$

as $n \longrightarrow \infty$. Let us define $C_{vv'} = \bigcap\limits_{i=1}^{r-1}\bigcap\limits_{j=1}^{r-1}\{A_{vv'}(i,j)\}$. Now, if $C_{vv'}$ is true for some $v, v' \in \{1, 2, \cdots, n\}$, according to (4.22), we have

$$\begin{aligned}
\widetilde{Cov_{vv'}} &= \frac{\sum\limits_{i=1}^{r-1}\sum\limits_{j=1}^{r-1} ij\widehat{M}_{vv'}(i,j)}{m} - \frac{\sum\limits_{i=1}^{r-1} i\widehat{M}_v(i)}{m}\frac{\sum\limits_{i=1}^{r-1} i\widehat{M}_{v'}(i)}{m} \\
&\le \frac{\sum\limits_{i=1}^{r-1}\sum\limits_{j=1}^{r-1} ij\left(mw_{vv'}(i,j) + m^{\frac{3}{4}}\right)}{m} - \frac{\sum\limits_{i=1}^{r-1} i\left(mw_v(i) - m^{\frac{3}{4}}\right)}{m}\frac{\sum\limits_{i=1}^{r-1} i\left(mw_{v'}(i) - m^{\frac{3}{4}}\right)}{m} \\
&= \sum_{i=1}^{r-1}\sum_{j=1}^{r-1} ijw_{vv'}(i,j) - \sum_{i=1}^{r-1} iw_v(i)\sum_{i=1}^{r-1} iw_{v'}(i) \\
&\qquad + \frac{r^2(r-1)^2}{4}m^{-\frac{1}{4}} + \frac{r(r-1)}{2}\sum_{i=1}^{r-1} i(w_v(i) + w_{v'}(i))m^{-\frac{1}{4}} - \frac{r^2(r-1)^2}{4}m^{-\frac{1}{2}} \\
&\le Cov_{vv'} + \frac{r^2(r-1)^2}{4}m^{-\frac{1}{4}} + \frac{r(r-1)}{2}\sum_{i=1}^{r-1} i(w_v(i) + w_{v'}(i))m^{-\frac{1}{4}} + \frac{r^2(r-1)^2}{4}m^{-\frac{1}{2}},
\end{aligned} \tag{4.27}$$

where $Cov_{vv'} = \sum\limits_{i=1}^{r-1}\sum\limits_{j=1}^{r-1} ijw_{vv'}(i,j) - \sum\limits_{i=1}^{r-1} iw_v(i)\sum\limits_{i=1}^{r-1} iw_{v'}(i)$. Similarly,

$$\widetilde{Cov_{vv'}} = \frac{\sum\limits_{i=1}^{r-1}\sum\limits_{j=1}^{r-1} ij\widehat{M}_{vv'}(i,j)}{m} - \frac{\sum\limits_{i=1}^{r-1} i\widehat{M}w(i)}{m}\frac{\sum\limits_{i=1}^{r-1} i\widehat{M}_{v'}(i)}{m}$$

$$
\begin{aligned}
&\geq \frac{\sum_{i=1}^{r-1} i\left(mw_v(i) - m^{\frac{3}{4}}\right)}{m} - \frac{\sum_{i=1}^{r-1} i\left(mw_v(i) + m^{\frac{3}{4}}\right)}{m}\frac{\sum_{i=1}^{r-1} i\left(mw_{v'}(i) + m^{\frac{3}{4}}\right)}{m} \\
&= Cov_{vv'} - \frac{r^2(r-1)^2}{4}m^{-\frac{1}{4}} - \frac{r(r-1)}{2}\sum_{i=1}^{r-1} i(w_v(i) + w_{v'}(i))m^{-\frac{1}{4}} - \frac{r^2(r-1)^2}{4}m^{-\frac{1}{2}}.
\end{aligned}
\tag{4.28}
$$

Now, by using (4.27) and (4.28), we have

$$
\left|\widetilde{Cov_{vv'}} - Cov_{vv'}\right| \leq \frac{r^2(r-1)^2}{4}m^{-\frac{1}{4}} + \frac{r(r-1)}{2}\sum_{i=1}^{r-1} i(w_v(i) + w_{v'}(i))m^{-\frac{1}{4}} + \frac{r^2(r-1)^2}{4}m^{-\frac{1}{2}}.
\tag{4.29}
$$

Let us define event $D_{vv'}$ as the event that (4.29) is valid, thus, we have shown, for all $v, v' \in \{1, 2, \cdots, n\}$, $C_{vv'} \subseteq D_{vv'}$, and consequently,

$$
\left\{\bigcap_{v=1}^{n}\bigcap_{v'=1}^{n}\{C_{vv'}\}\right\} \subseteq \left\{\bigcap_{v=1}^{n}\bigcap_{v'=1}^{n}\{D_{vv'}\}\right\}.
$$

As a result,

$$
\mathbb{P}\left(\bigcap_{v=1}^{n}\bigcap_{v'=1}^{n}\{D_{vv'}\}\right) \geq \mathbb{P}\left(\bigcap_{v=1}^{n}\bigcap_{v'=1}^{n}\{C_{vv'}\}\right).
$$

Thus, by using (4.26), we have

$$
\mathbb{P}\left(\bigcap_{v=1}^{n}\bigcap_{v'=1}^{n}\{D_{vv'}\}\right) \longrightarrow 1,
$$

as $n \longrightarrow \infty$. Hence, with high probability, for all $v, v' \in \{1, 2, \cdots, n\}$, we have

$$
\left|\widetilde{Cov_{vv'}} - Cov_{vv'}\right| \leq \frac{r^2(r-1)^2}{4}m^{-\frac{1}{4}} + \frac{r(r-1)}{2}\sum_{i=1}^{r-1} i(w_v(i) + w_{v'}(i))m^{-\frac{1}{4}} + \frac{r^2(r-1)^2}{4}m^{-\frac{1}{2}}.
\tag{4.30}
$$

Thus, we can conclude, with high probability, for all $v, v' \in \{1, 2, \cdots, n\}$, $\widetilde{Cov_{vv'}}$'s are close to $Cov_{vv'}$'s.

Now, if (u, u') is an inter-community edge, the adversary knows $Cov_{uu'} \leq \epsilon_1$, and as a result, $Cov_{vv'} \leq \epsilon_1$, thus, the adversary removes that edge. Now, we can conclude $(v, v') \notin \widetilde{F}$, and in other words, $(\Pi(u), \Pi(u')) \notin \widetilde{F}$. This is true with high probability, simultaneously for all $u, u' \in \{1, 2, \cdots, n\}$ where (u, u') is an inter-community edge.

In addition, if (u, u') is an intra-community edge, the adversary knows $Cov_{uu'} \geq \epsilon_2$, and as a result, $Cov_{vv'} \geq \epsilon_2$. Now, we can conclude $(v, v') \in \widetilde{F}$, and in other words, $(\Pi(u), \Pi(u')) \in \widetilde{F}$. This is true with high probability, simultaneously for all $u, u' \in \{1, 2, \cdots, n\}$ where (u, u') is an intra-community edge.

As a result, for large enough n, we have $\mathbb{P}\left(\widetilde{G} \simeq G\right) \to 1$, so the adversary can reconstruct the association graph of the anonymized version of the data which is based on a threshold with an arbitrarily small error probability. □

Now, the adversary has a graph structure shown in Figure 4.6b, where subgraph G_1 is a connected graph with s_1 vertices which is disjoint from the reminder of the association graph ($G' = G - G_1$). In other words,

$$G = G_1 \cup G'.$$

Now, we can repeat the same reasoning as that in the proof of Theorem 7, Theorem 8, Theorem 9, and Theorem 10 to obtain the same results for this case.

Discussion 7: The stochastic block model is a generative model for random graphs [1, 2, 49, 58, 86, 90, 121]. Note that there are two key differences between the stochastic block model and the work here. First, in the stochastic block model, the edge set is sampled at random and the probability distributions of edges are the key part of the work, while here the analysis is based on the users' data traces, and the statistical knowledge of the adversary is a key part. Second, in the stochastic block model, nodes within a community connect to nodes in other communities in an equivalent way. In other words, any two vertices $u \in C_i$ and $v \in C_j$ are connected by an edge with probability p_{ij}, where C_i and C_j are different blocks, so all edges between two communities have the same weights or strengths. While here, as shown in Figure 4.6a, there is no need that the inter-community edges, corresponding to the covariance of nodes in separate communities, has the same value as others; in other words, there is no need for the nodes in a community to connect to the nodes in other communities in an equivalent way. In our work, for each of intra-community edges, $Cov_{uu'} \geq \epsilon_2$, and for each of inter-community edges, $Cov_{uu'} \leq \epsilon_1$, thus, edges have different weights.

4.6 Improving Privacy in the Presence of Dependency

In the previous parts of this chapter, we argued and demonstrated that inter-user dependency degrades the privacy provided by standard privacy-preserving mechanisms (PPMs). In this section, we discuss how to design PPMs considering inter-user dependency in order to better preserve privacy. First, note that independent obfuscation alone cannot be sufficient even at a high noise level, because it cannot change the association graph. Therefore, the adversary can still reconstruct the association graph with a small number of observations if we add independent obfuscation noise. To mitigate this issue, we suggest that associated users collaborate in applying the noise when deploying a PPM.

For clarity, we focus on the two-state i.i.d. case ($r = 2$). In the first part, we also focus on the case the association graph consists of subgraphs with the size of each of them less than or equal to 2 ($s_l \leq 2$). Thus, according to Figure 4.7, there are some connected users and there are also some isolated users. First, we state the following lemma.

Lemma 9. Let $X_u(k) \sim \text{Bernoulli}(p_u)$ and $X_{u'}(k) \sim \text{Bernoulli}(p_{u'})$; then, there exists an obfuscation technique with a noise level equal to

$$\breve{a}(u,u') = \frac{\text{Cov}(X_u(k), X_{u'}(k))}{\max\{p_u, p_{u'}, 1 - p_u, 1 - p_{u'}\}},$$

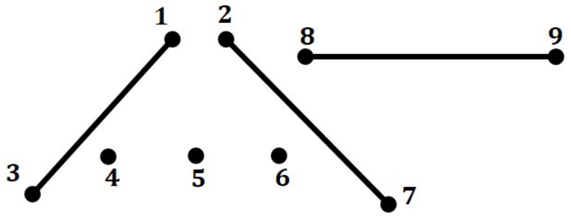


Figure 4.7: Graph G consists of some subgraphs (G_l) with $s_l \leq 2$.

for the dataset of user u and user u' such that $\check{Z}_u(k)$ and $\check{Z}_{u'}(k)$ are independent from each other. Note $\check{Z}_u(k)$ and $\check{Z}_{u'}(k)$ are the k^{th} (reported) data point of user u and u', respectively, after applying obfuscation with the noise level equal to $\breve{a}(u, u')$.

Proof. Let $X_u(k) \sim \text{Bernoulli}(p_u)$ and $X_{u'}(k) \sim \text{Bernoulli}(p_{u'})$. Then, to make these two sequences independent, it suffices if $\check{Z}_u(k)|\check{Z}_{u'}(k) = 0$ has the same distributions as $\check{Z}_u(k)|\check{Z}_{u'}(k) = 1$. We only prove for the case $\max\{p_u, p_{u'}, 1-p_u, 1-p_{u'}\} = 1-p_{u'}$, and the proofs of the other cases are similar to this one. Now, If $X_u(k) = 1$ and $X_{u'}(k) = 1$, we pass $X_u(k)$ through a $BSC(\Upsilon)$ in order to obtain $\check{Z}_u(k)$. Thus,

$$\frac{\mathbb{P}\left(X_u(k) = 1, X_{u'}(k) = 0\right)}{1 - p_{u'}} = \frac{\mathbb{P}\left(X_u(k) = 1, X_{u'}(k) = 1\right)(1-\Upsilon)}{p_{u'}},$$

and Υ can be calculated as

$$\Upsilon = 1 - \frac{p_{u'}}{1-p_{u'}} \frac{\mathbb{P}\left(X_u(k) = 1, X_{u'}(k) = 0\right)}{\mathbb{P}\left(X_u(k) = 1, X_{u'}(k) = 1\right)}.$$

Now, we can conclude,

$$\begin{aligned}
&\breve{a}(u, u') = \Upsilon \mathbb{P}\left(X_u(k) = 1, X_{u'}(k) = 1\right) \\
&= \left(1 - \frac{p_{u'}}{1-p_{u'}} \frac{\mathbb{P}\left(X_u(k) = 1, X_{u'}(k) = 0\right)}{\mathbb{P}\left(X_u(k) = 1, X_{u'}(k) = 1\right)}\right) \mathbb{P}\left(X_u(k) = 1, X_{u'}(k) = 1\right) \\
&= \mathbb{P}\left(X_u(k) = 1, X_{u'}(k) = 1\right) - \frac{p_{u'}}{1-p_{u'}} \mathbb{P}\left(X_u(k) = 1, X_{u'}(k) = 0\right) \\
&= \frac{\mathbb{P}\left(X_u(k) = 1, X_{u'}(k) = 1\right) - p_{u'}\left(\mathbb{P}\left(X_u(k) = 1, X_{u'}(k) = 1\right) + \mathbb{P}\left(X_u(k) = 1, X_{u'}(k) = 0\right)\right)}{1-p_{u'}}
\end{aligned}$$

$$= \frac{\mathbb{P}\left(X_u(k) = 1, X_{u'}(k) = 1\right) - p_u p_{u'}}{1 - p_{u'}}$$
$$= \frac{\mathrm{Cov}(X_u(k), X_{u'}(k))}{\max\{p_u, p_{u'}, 1 - p_u, 1 - p_{u'}\}}.$$

Now, we want to explain the idea behind this lemma by an example.

Example 3. Let $X_u(k) \sim \text{Bernoulli}\left(\frac{3}{5}\right)$ and $X_{u'}(k) \sim \text{Bernoulli}\left(\frac{1}{5}\right)$, and let Table 4.1 show the joint probability mass function of $X_u(k)$ and $X_{u'}(k)$.

Table 4.1: Joint probability mass function of $X_u(k)$ and $X_{u'}(k)$.

$X_{u'}(k)$ $X_u(k)$	0	1
0	$\frac{7}{20}$	$\frac{1}{20}$
1	$\frac{9}{20}$	$\frac{3}{20}$

As a result, if we observe 2000 bits of data, Table 4.2a shows the expected results according to Table 4.1.

Then, to make $\check{Z}_u(k)$ and $\check{Z}_{u'}(k)$ independent, it is sufficient for $\check{Z}_u(k)|\check{Z}_{u'}(k) = 0$ to have the same distribution as $\check{Z}_u(k)|\check{Z}_{u'}(k) = 1$. This means we should have

$$\frac{\mathbb{P}\left(\check{Z}_u(k) = 1, \check{Z}_{u'}(k) = 1\right)}{\mathbb{P}\left(\check{Z}_{u'}(k) = 1\right)} = \frac{\mathbb{P}\left(\check{Z}_u(k) = 1, \check{Z}_{u'}(k) = 0\right)}{\mathbb{P}\left(\check{Z}_{u'}(k) = 0\right)};$$

thus, according to Table 4.2b,

$$\frac{300(1 - \Upsilon)}{100 + 300} = \frac{900}{700 + 900} \rightarrow \Upsilon = \frac{1}{4},$$

where Υ is the portion of data points $X_u(k)$ that need to be flipped in the fourth region of Table 4.2a (i.e., the region $X_u(k) = 1, X_{u'}(k) = 1$). Now, we need to change $\frac{1}{4} \cdot 300 = 75$ of data bits. As a result, if $X_u(k) = 1$ and $X_{u'}(k) = 1$, then, we pass $X_u(k)$ through a $BSC(\frac{1}{4})$, and obtain $\check{Z}_u(k)$. Hence, asymptotic noise level is equal to

$$\check{a}(u, u') = \frac{3}{20} \cdot \frac{1}{4} = 3.75\%.$$

Table 4.2: (a) The expected results of $X_u(k)$ and $X_{u'}(k)$ according to Table 4.1 after observing 2000 bits of data, and (b) The desired results to make $\check{Z}_u(k)$ and $\check{Z}_{u'}(k)$ independent from each other.

(a)

$X_{u'}(k)$ $X_u(k)$	0	1
0	700	100
1	900	300

(b)

$\check{Z}_{u'}(k)$ $\check{Z}_u(k)$	0	1
0	700	175
1	900	225

It is easy to check that the asymptotic noise level will be given by the equation in Lemma 9. Specifically, for the above example,

$$\text{Cov}(X_u(k), X_{u'}(k)) = \mathbb{P}(X_u(k) = 1, X_{u'}(k) = 1) - \mathbb{P}(X_u(k) = 1)\mathbb{P}(X_{u'}(k) = 1) = \frac{3}{20} - \frac{3}{5} \cdot \frac{1}{5} = \frac{3}{100},$$

and we have

$$\check{a}(u, u') = \frac{\text{Cov}(X_u(k), X_{u'}(k))}{\max\{p_u, p_{u'}, 1 - p_u, 1 - p_{u'}\}} = \frac{\frac{3}{100}}{\frac{4}{5}} = 3.75\%.$$

□

Lemma 9 provides a method to convert correlated data to independent traces. The remaining task is to show that we can achieve perfect privacy after applying such a method. As shown in Figure 4.8, two stages of obfuscation and one stage of anonymization are employed to achieve perfect privacy for users. Note that the first stage of obfuscation is due to Lemma 9 and the second stage (as will be explained in Theorem 11) is the same obfuscation technique given in Theorem 1 of Chapter 2. In Figure 4.8, $\check{Z}_u(k)$ shows the (reported) data point of user u at time k after applying the first stage of obfuscation with the noise level equal to

$$\check{a}(u,u') = \frac{\mathrm{Cov}(X_u(k), X_{u'}(k))}{\max\{p_u, p_{u'}, 1-p_u, 1-p_{u'}\}}$$

for the dataset of user u and user u', $Z_u(k)$ shows the (reported) data point of user u at time k after applying the second stage of obfuscation with the noise level equal to

$$a_n = c' n^{-\left(\frac{1}{s}-\beta\right)},$$

and $Y_u(k)$ shows the (reported) data point of user u at time k after applying anonymization.

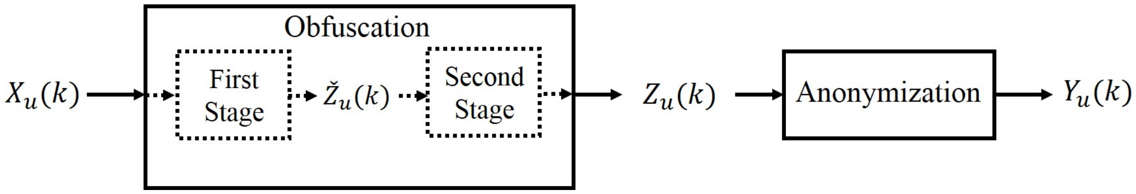


Figure 4.8: The sequence $Z_u(k)$, $k = 1, 2, \ldots, m$, is the obfuscated version of $X_u(k)$, $k = 1, 2, \ldots, m$, and the sequence $Y_u(k)$, $k = 1, 2, \ldots, m$, is observed by the adversary after $X_u(k)$, $k = 1, 2, \ldots, m$, is obfuscated and anonymized.

Consider $G(\mathcal{V}, F)$, where $s_l \leq 2$. We have the same model for p_u as in the previous sections: p_u is chosen from some density $f_P(p_u)$ such that, for $\delta_1, \delta_2 > 0$:

$$\begin{cases} \delta_1 < f_P(p_u) < \delta_2, & p_u \in (0,1). \\ f_P(p_u) = 0, & p_u \notin (0,1). \end{cases}$$

Also, if $(u,u') \in F$, $\rho_{uu'}$ is chosen according to some density $f_P(\rho_{uu'}|p_u,p_{u'})$ with range of $\left[0, \min\left\{\sqrt{\frac{p_u(1-p_{u'})}{p_{u'}(1-p_u)}}, \sqrt{\frac{p_{u'}(1-p_u)}{p_u(1-p_{u'})}}\right\}\right]$. The following theorem states that we can indeed achieve perfect privacy if we allow collaboration between users.

Theorem 11. For the two-state model, if $\mathbf{Z}$ is the obfuscated version of $\mathbf{X}$, $\mathbf{Y}$ is the anonymized version of $\mathbf{Z}$, and the size of all subgraphs are less than or equal to 2, there exists an anonymization/obfuscation scheme such that for all $(u,u') \in F$, the asymptotic noise level for users u and u' is at most

$$a(u,u') = \frac{\text{Cov}(X_u(k), X_{u'}(k))}{\max\{p_u, p_{u'}, 1-p_u, 1-p_{u'}\}},$$

to achieve perfect privacy for all users. The anonymization parameter $m = m(n)$ can be made arbitrarily large.

Proof. There are two main steps.

Step 1: De-correlate based on Lemma 9. In particular, note that for at least half of the users, no noise is added in this step. More specifically, define

$$\mathcal{U} = \text{Set of unaffected users} = \{u : \text{no noise is added to user } u \text{ in this step}\}.$$

Then after step 1, we have $\check{Z}_u(k) \sim \text{Bernoulli}(\check{q}_u)$. As a result,

- For $u \in \mathcal{U}$; $\check{Z}_u(k) = X_u(k)$ and $\check{q}_u = p_u$.

- For $u \in \{1, 2, \cdots, n\} - \mathcal{U}$; $\check{Z}_u(k) \neq X_u(k)$ and $\check{q}_u \neq p_u$.

Note $|\mathcal{U}| \geq \frac{n}{2}$, because the main graph consists of some subgraphs with $s_l \leq 2$.

Step 2: Assume $\check{q}_u$'s are known to the adversary. The setup is now very similar to Theorem 1 in Chapter 2, where perfect privacy is proved for the i.i.d. data. But there is a difference here. Specifically, although the users' data $\check{Z}_u(k)$ are now independent, the distribution of $\check{q}_u$'s are not, since they are the result of the data-dependent obfuscation technique of Lemma 9. Luckily, this issue can be easily resolved so that we can show perfect privacy for user 1. The main idea is to use the fact that as stated above, at least $\frac{n}{2}$ of the users are not impacted by the de-correlation step. As we see below, these users will be sufficient to ensure perfect privacy for user 1 (which may or may not be in the set $\mathcal{U}$).

Let us explore the distributions of $\check{Q}_u = \check{q}_u$ for users in the set $\mathcal{U}$. For any correlated pair of users, the method of Lemma 9 leaves the one whose p_u is farthest from $\frac{1}{2}$ intact. Since p_u's are chosen independently from each other and each user is correlated with only one user, it is easy to see that for users in the set $\mathcal{U}$, the $\check{q}_u$'s are i.i.d. with the following probability density function

$$f_{\check{Q}}(\check{q}_u) = 2 f_P(\check{q}_u) \int_{\min(\check{q}_u, 1-\check{q}_u)}^{\max(\check{q}_u, 1-\check{q}_u)} f_P(x) dx.$$

Therefore, the setup is the same as Theorem 1 in Chapter 2 where we want to prove perfect privacy for user 1, and we have $\frac{n}{2}$ users who are independent from user 1 and their parameter $\check{q}_u$ is chosen i.i.d. according to a density function. However, we need to check that the density function $f_{\check{Q}}(\check{q})$ satisfies the condition $\check{\delta}_1 < f_{\check{Q}}(\check{q}_u) < \check{\delta}_2$ for some $\check{\delta}_1$ and $\check{\delta}_2$ on a neighborhood $\check{q}_u \in [p_u - \epsilon', p_u + \epsilon']$. First, note that

$$\begin{aligned} f_{\check{Q}}(\check{q}_u) &= 2 f_P(\check{q}_u) \int_{\min(\check{q}_u, 1-\check{q}_u)}^{\max(\check{q}_u, 1-\check{q}_u)} f_P(x) dx. \\ &< 2\delta_2^2 = \check{\delta}_2. \end{aligned}$$

Next,

$$\begin{aligned} f_{\check{Q}}(\check{q}_u) &= 2 f_P(\check{q}_u) \int_{\min(\check{q}_u, 1-\check{q}_u)}^{\max(\check{q}_u, 1-\check{q}_u)} f_P(x) dx. \\ &> 2\delta_1^2 |1 - 2\check{q}_u| = \check{\delta}_1. \end{aligned}$$

Thus, as long as $p_u \neq \frac{1}{2}$, the condition is satisfied [3]. Therefore, we can show perfect privacy for user 1. Note that here, in the second step, we need to apply a second stage of obfuscation and apply anonymization according to Theorem 1 in Chapter 2. Nevertheless, since the noise level $a_n \to 0$ for this second stage, the asymptotic noise level will stay the same as that for step 1, i.e.

$$a(u,u') = \breve{a}(u,u') = \frac{|\mathrm{Cov}(X_u(k), X_{u'}(k))|}{\max\{p_u, p_{u'}, 1-p_u, 1-p_{u'}\}}.$$

□

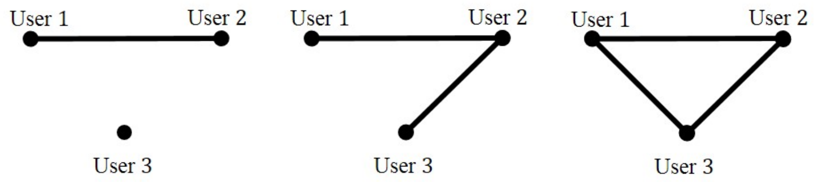
Now, the above method can be extended to the case where $s_l > 2$. Let $s_l = 3$. From Figure 4.9, there are two different situations in this case:

1. Case 1: As shown in Figure 4.9b, user 1 and user 2 are correlated, and user 2 and user 3 are correlated. In the first step, we de-correlate user 2 and user 3 based on Lemma 9. Now, we face a similar situation as that in the case $s_l = 2$ (as shown in Figure 4.9a), and we de-correlate them based on Lemma 9. Hence, we can make all of the users independent from each other and then according to Theorem 11, we can achieve perfect privacy for all of them.

2. Case 2: As shown in Figure 4.9c, all three users are correlated to each other. In the first step, we use Lemma 9 to make user 1 and user 3 uncorrelated. Now, we have a similar situation as case 1, so we can make all the users independent from each other and then, according to Theorem 11, we can achieve perfect privacy for all of them.

Discussion 8: Note that obfuscating data by adding non-zero asymptotic noise may degrade utility significantly. Therefore, in practice, it is usually not possible to de-correlate *all*

[3] The case $p_u = \frac{1}{2}$ has zero probability, and thus need not be considered. Nevertheless, the result can be shown for $p_u = \frac{1}{2}$, as all we require is a number of users proportional to the length of the interval in the vicinity of p_u.



(a) $s_l = 2$. (b) $s_l = 3$: Case 1. (c) $s_l = 3$: Case 2.

Figure 4.9: Three different ways which 3 users can be correlated to each other.

Table 4.3: Summary of the results for the case anonymization is employed as a PPM for "no privacy" as a function of number of adversary's observations per user (m). Here, s is the size of group of users whose data traces are dependent, r is the number of possible values for each user's data point, $|E|$ is the size of set of edges in the Markov chain, and the results hold for any $\alpha > 0$.

Users' data model	Independent users [73]	Dependent users
	m	m
Two-state i.i.d. model	$\Omega\left(n^{2+\alpha}\right)$	$\Omega\left(n^{\frac{2}{s}+\alpha}\right)$
r-state i.i.d. model	$\Omega\left(n^{\frac{2}{r-1}+\alpha}\right)$	$\Omega\left(n^{\frac{2}{s(r-1)}+\alpha}\right)$
r-state Markov chain model	$\Omega\left(n^{\frac{2}{\lvert E\rvert-r}+\alpha}\right)$	$\Omega\left(n^{\frac{2}{s(\lvert E\rvert-r)}+\alpha}\right)$

dependent users without imposing substantial utility degradation. In addition, in order to convert correlated data to independent data, users should collaborate together and disclose their private data to each other, which degrades privacy unless users trust each other. In such a setting, a possible approach in applying our technique is to only add de-correlation noise to the data of highly-dependent users (e.g., spouses and close friends), and leave data of less-dependent users (e.g., co-workers) unchanged.

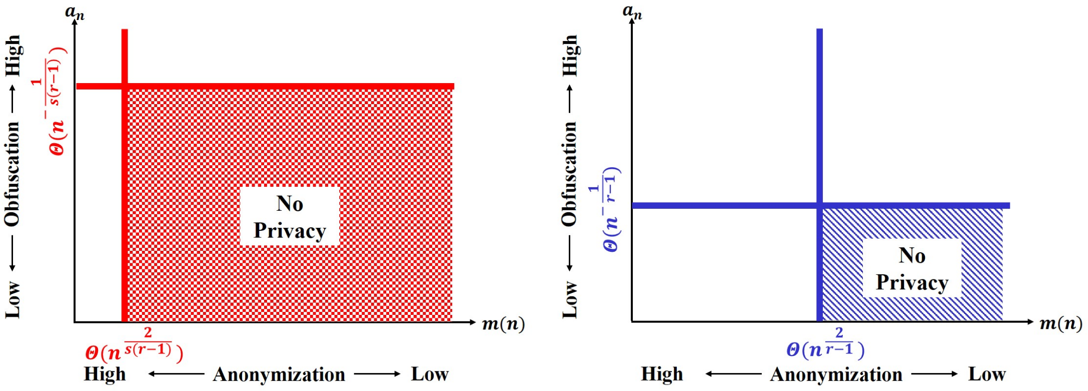
Table 4.4: Summary of the results for the case both obfuscation and anonymization are combined to be employed as a PPM for "no privacy" as a function of number of adversary's observations per user (m) and the amount of noise level (a_n). Here, s is the size of group of users whose data traces are dependent, r is the number of possible values for each user's data point, $|E|$ is the size of set of edges in the Markov chain, and the results hold for any $\alpha > 0$.

Users' data model	Independent users Chapter 2		Dependent users	
	m	a_n	m	a_n
Two-state i.i.d. model	$\Omega\left(n^{2+\alpha}\right)$	$O\left(n^{-1-\beta}\right)$	$\Omega\left(n^{\frac{2}{s}+\alpha}\right)$	$O\left(n^{-\frac{1}{s}-\beta}\right)$
r-state i.i.d. model	$\Omega\left(n^{\frac{2}{r-1}+\alpha}\right)$	$O\left(n^{-\frac{1}{r-1}-\beta}\right)$	$\Omega\left(n^{\frac{2}{s(r-1)}+\alpha}\right)$	$O\left(n^{-\frac{1}{s(r-1)}-\beta}\right)$
r-state Markov chain model	$\Omega\left(n^{\frac{2}{\vert E\vert-r}+\alpha}\right)$	$O\left(n^{-\frac{1}{\vert E\vert-r}-\beta}\right)$	$\Omega\left(n^{\frac{2}{s(\vert E\vert-r)}+\alpha}\right)$	$O\left(n^{-\frac{1}{s(\vert E\vert-r)}-\beta}\right)$

4.7 Summary of the Results

Consider a setting with n total users. As in Chapter 2, privacy depends on two parameters: (1) $m = m(n)$, the number of data points after which the pseudonyms of users are changed in the anonymization technique, i.e., smaller m implies higher levels of anonymization; and (2) a_n, which indicates the amplitude of the obfuscation noise, i.e., larger a_n implies higher levels of obfuscation.

When there are a large number of users in the setting ($n \rightarrow \infty$) and each user's dataset is governed by an i.i.d. process with r possible values for each data point (e.g., r possible locations), we obtain a no-privacy region in the $m(n) - a_n$ plane. Figure 4.10a shows the no-privacy region for the case when there exists inter-user dependency, and Figure 4.10b shows the no-privacy region when the users' traces are independent across users. There exists a larger no-privacy region in the presence of inter-user dependency; therefore, we find that dependency between users weakens their privacy.



(a) The dependent case.

(b) The independent case.

Figure 4.10: Representations of the no-privacy region in the case of dependent and independent users. Note that $m(n)$ is the number of the adversary's observations per user (degree of anonymization), and a_n is the amount of noise level (degree of obfuscation). Here, the size of the group of users whose data traces are dependent is equal to s.

In addition, for the case where users' datasets are governed by an irreducible and aperiodic Markov chains with r states and $|E|$ edges, we obtain similar results, again showing that inter-user dependency degrades user privacy.

The summary of the results is also shown in Tables 4.3 and 4.4.Note that for only anonymization case, an initial extension in Gaussian case with known covariance matrix is also presented in [114].

CHAPTER 5

LEVERAGING PRIOR KNOWLEDGE ASYMMETRIES IN THE DESIGN OF IOT PRIVACY-PRESERVING MECHANISMS

5.1 Introduction

Emerging technologies such as the Internet of Things (IoT) [31] promise to revolutionalize users' lives by adapting to each user's specific needs and habits as gleaned from their data traces. However, this necessitates that the data of an immense number of users are interconnected, thus posing intrinsic threats to user privacy and leaving sensitive information vulnerable [85]. There has been significant work on privacy-preserving mechanisms (PPMs) [6, 10, 18, 30, 33, 39, 40, 45, 71, 74, 96, 99, 102]. These PPMs can largely be categorized into two groups: anonymization and obfuscation. Anonymization techniques enhance privacy by removing the information that discloses the personal identity from data sets [18, 33, 45, 71, 74, 96, 102]. In contrast, obfuscation techniques enhance privacy by using misleading, false, or ambiguous information [6, 10, 30, 39, 40, 99]. These two classes of techniques have one common problem: that they degrade system's utility to enhance privacy [29, 99].

Recently, a new method termed "remapping", which is similar to posterior data processing in database systems, has emerged as an effective method to exploit asymmetries in the privacy problem to substantially improve system utility without a corresponding loss in privacy for a PPM that employs obfuscation [12]. In particular, remapping is employed in scenarios where a friend (e.g. an IoT application) exists that does not have prior statistical information about user behavior, whereas the adversary in the environment has perfect

The work presented in this chapter was submitted in [113].

statistical information about the user's behavior. This may occur, for example, when each intended recipient is either naive or only looking at a single datum or small set of data from the user, whereas the adversary is sophisticated and has access to data across a large time period from the user.

In such a case, the adversary can use their statistical advantage to obtain a better estimate of the user's data than the friend. Remapping recognizes this fact and reveals a more accurate version of the data that the adversary would have been able to obtain anyway using their statistical advantage, so there is no loss in privacy, but which will improve the accuracy for the user's friend. Hence, by recognizing this asymmetry, utility has been improved at no loss in privacy versus a scheme that did not do remapping; a simple example of the mechanism is demonstrated in Section II. Not surprisingly, this approach has garnered a growing amount of interest in the privacy community [51, 72, 79, 80, 82], hence motivating a more fundamental analysis.

Here, we take the first information-theoretic look at this remapping technique. We introduce a simple information-theoretic model to explain how the utility can be improved without a loss in privacy. Next, we employ our model to explore important aspects of remapping that have not been considered. As acknowledged briefly in [12], a risk of remapping is that it relies critically on accurate knowledge of the adversary's statistical model. In particular, if the adversary does not have accurate statistical information and the user employs remapping, we discuss that privacy is compromised in two separate ways: (i) the adversary obtains a more accurate version of the data than they would have had without remapping; and (ii) the adversary is able to improve their statistical knowledge of the users' data beyond what they would have been able to do without remapping. Interestingly, we will see that the second type of leakage is increased if the obfuscation noise is increased. We provide the first analysis of the loss of privacy due to each of these factors.

After analyzing the loss in privacy under standard remapping [12], we next turn to countermeasures. We introduce a random remapping algorithm, where data points are independently remapped with some probability. For a given utility for the intended recipient, this approach greatly complicates model improvement at the adversary versus deterministic remapping approaches, thus it improves the privacy-utility trade-off.

The rest of this chapter is organized as follows. In Section 5.2, we present the framework: system model, metrics, and definitions. We next demonstrate in Section 5.3 how the current remapping technique proposed by [12] increases utility while satisfying the same level of privacy if the adversary has the *perfect prior*. In Section 5.4, we quantify information leakage caused by the mentioned remapping technique [12] if the adversary does not have a perfect prior. In particular, we show that leakage about the distribution of true data is a serious issue. Motivated by this, in Section 5.5 we propose our new method called "*Randomized Remapping*" to improve the privacy for a given utility in this situation. This method provides a trade-off between leakage of distribution of true data and the utility.

5.2 System Model, Definitions, and Metrics

We assume a system with one user who creates a length-m sequence $\mathbf{X}$ of data:

$$\mathbf{X} = [X(1), X(2), \cdots, X(m)],$$

where $X(k)$ denotes the user's true data at time k which should be protected from a potential adversary. To preserve the privacy of the user's true data, the obfuscated data is obtained by adding noise ($\mathbf{W}$) to ($\mathbf{X}$). In other words, the reported noisy version of data ($\mathbf{Y}$) is obtained as $\mathbf{Y} = \mathbf{X} + \mathbf{W}$, where

$$\mathbf{W} = [W(1), W(2), \cdots, W(m)].$$

$$\mathbf{Y} = [Y(1), Y(2), \cdots, Y(m)].$$

As shown in Figure 5.1, there exists an “intended” friend (e.g., an IoT application) who doesn't have prior statistical knowledge about the user behavior and a “sophisticated” adversary who has knowledge about the prior behavior of the user (π_{Adv}). The adversary

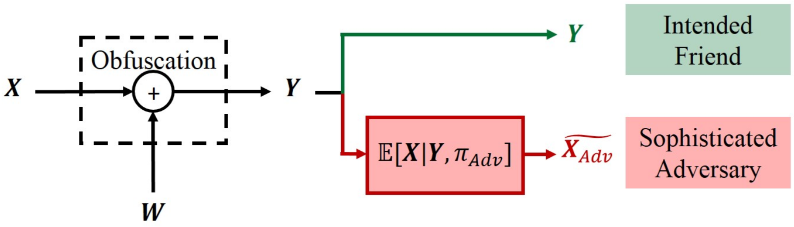


Figure 5.1: System Model: Case where additive obfuscation (without remapping) is applied to the user's data points. The (naive) intended friend does not have a prior distribution for $\mathbf{X}$ and hence employs $\mathbf{Y}$ for the user's data. A sophisticated adversary, who possesses a prior distribution for $\mathbf{X}$, can use this prior to obtain a better estimate of the user's data.

observes the noisy reported data $\mathbf{Y}$ and uses it to find the estimate $\widetilde{\mathbf{X}}_{Adv}$, which denotes the estimate of the adversary given her observed data ($\mathbf{Y}$) and her knowledge of the prior about the user (π_{Adv}) as $\widetilde{\mathbf{X}}_{Adv} = \mathbb{E}[\mathbf{X}|\mathbf{Y}, \pi_{Adv}]$. As a result, there exist asymmetries in knowledge and/or sophistication between the intended friend and the adversary. The remapping technique, which is introduced by Chatzikokolakis et al. [12], exploits these asymmetries to publish a more accurate version of data that the sophisticated adversary would have been able to obtain anyway. As shown in Figure 5.2, each reported data is remapped into the best possible data point according to the perfect prior information of the adversary.

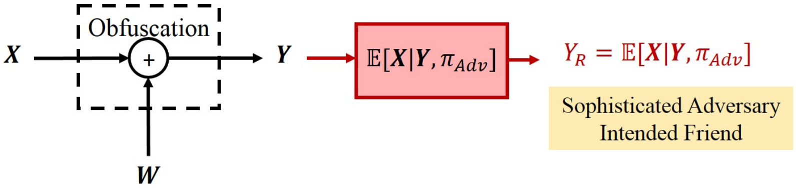


Figure 5.2: Remapping: $\mathbf{X}$ is the user's true data, $\mathbf{W}$ is the amount of noise added through the obfuscation process, $\mathbf{Y}$ is the noisy reported data after applying obfuscation, and $\mathbf{Y}_R$ is the remapped data which is the best possible estimate of the adversary according to her perfect prior knowledge about the user.

Data Sample Model: We adopt a Gaussian model that facilitates analysis. User traces are assumed to be independent and identically distributed (i.i.d.) Gaussian series, and each data point is drawn from a normal distribution with mean μ variance σ_s^2, $X(k) \sim \mathcal{N}\left(\mu, \sigma_s^2\right)$.

We also assume there exists some underlying prior for the distribution of the mean (μ); we also take this to be Gaussian, and hence assume $\mu \sim \mathcal{N}\left(0, \sigma_{\mu}^{2}\right)$.

Obfuscation Mechanism: The obfuscated data is obtained by passing the data through an additive white Gaussian noise (AWGN) channel. Hence, $\mathbf{Y}$, the reported data of the user, is the sum of the true data, $\mathbf{X}$, and the noise, $\mathbf{W}$, where all $W(k)$ are i.i.d. with respect to time and are drawn from a zero-mean normal distribution with variance equal to σ_{w}^{2}. Thus, we have

$$Y = X + W \sim \mathcal{N}\left(\mu, \sigma_{s}^{2} + \sigma_{w}^{2}\right).$$

Sophisticated Adversary Model: Here, the adversary logs the user's data over time to generate a prior about the behavior of the user and performs an inference attack to estimate the best possible data given this generated prior. Note that the remapping literature [12] has considered a *perfect prior* for the adversary. In reality, the adversary, however strong, cannot have exact knowledge of the user's whereabouts, so she cannot build the perfect prior. In this paper, different adversarial settings have been considered: in Section 5.3, we assume an adversary with perfect prior, and in Section 5.4, we assume an adversary with imperfect prior. It is critical to note that the adversary knows the mechanism of the obfuscation, but she does not know the exact value of the noise which will be added during obfuscation and does not have any other auxiliary information or side information about user's data.

Remapping Mechanism: In the absence of remapping, and given the *perfect prior* for the adversary, the adversary can estimate $\mathbf{X}$, using the reported noisy version of the data ($\mathbf{Y}$) as:

$$\mathbf{Y}_{R} = \mathbb{E}\left[\mathbf{X}|\mathbf{Y}, \mu\right] = \frac{\sigma_{w}^{2}}{\sigma_{s}^{2} + \sigma_{w}^{2}}\mu + \frac{\sigma_{s}^{2}}{\sigma_{s}^{2} + \sigma_{w}^{2}}\mathbf{Y}, \tag{5.1}$$

where $\mathbf{Y}_R$ is the estimate of the adversary given the observed data ($\mathbf{Y}$) and her perfect knowledge of the prior (π_{Adv}). Remapping simply notes that, since the adversary obtains $\mathbf{Y}_R$ anyway (as shown in Figure 5.2), we might as well provide it to the applications to improve the utility [12].

Metrics: Here, the mean squared error (MSE) is employed as a metric to quantify both utility degradation and privacy (In Appendix 5.6, we also include mutual information as a measure of privacy leakage). In this paper, " $\mathcal{UD}$ " denotes the MSE of the intended application/friend which quantifies utility degradation. Also, " $\mathcal{P}$ " denotes the MSE of the adversary about the true data and " $\grave{\mathcal{P}}$ " denotes the MSE of the adversary about the distribution of the true data. Note that both " $\mathcal{P}$ " and " $\grave{\mathcal{P}}$ " quantify the level of privacy.

5.3 Case 1: Perfect Knowledge of the Adversary

In this section, we assume the adversary knows the exact value of the mean (μ).

5.3.1 Without Remapping Technique

Without remapping, the user's intended friend, which is oblivious to the prior knowledge of the user, observes only the noisy data (Y). Thus, the MSE of the application which quantifies the utility degradation can be calculated as:

$$\mathcal{UD}_{NR}^{(I)} = \mathbb{E}\left[\left(\widetilde{X}_{App} - X\right)^2\right] = \mathbb{E}\left[(Y - X)^2\right] = \sigma_w^2. \tag{5.2}$$

In comparison to the user's friend, the sophisticated adversary obtains $\widetilde{X}_{Adv} = \mathbb{E}[X|Y, \mu]$. As a result, the MSE of the adversary which quantifies the level of privacy is calculated as:

$$\mathcal{P}_{NR}^{(I)} = \mathbb{E}\left[\left(\widetilde{X}_{Adv} - X\right)^2\right] = \mathbb{E}\left[(Y_R - X)^2\right] = \frac{\sigma_w^2 \sigma_s^2}{\sigma_s^2 + \sigma_w^2}. \tag{5.3}$$

5.3.2 With Remapping Technique

In this case, both the adversary and the user's friend observe the same reported data, $\widetilde{X}_{Adv} = \widetilde{X}_{App} = Y_R = \mathbb{E}[X|Y,\mu]$. Now, the MSE of the adversary and the MSE of the application are equal and can be quantified as:

$$\mathcal{UD}_R^{(I)} = \mathcal{P}_R^{(I)} = \mathbb{E}\left[(Y_R - X)^2\right] = \frac{\sigma_w^2\sigma_s^2}{\sigma_s^2 + \sigma_w^2}. \tag{5.4}$$

Since the intended friend/application is oblivious to the prior statistical knowledge about the user behavior, the MSE of the adversary is always smaller than or equal to the MSE of the application ($\mathcal{P} \leq \mathcal{UD}$). From Sections 5.3.1 and 5.3.2, we can conclude the remapping technique provides the best utility among techniques satisfying the same level of privacy in the case of perfect knowledge of the adversary [12].

5.4 Case 2: Imperfect Knowledge of the Adversary

Here, we assume the adversary has a noisy version of the prior information, as might be obtained from a learning set of limited length. Specifically, the adversary has $\breve{\mu} = \mu + E$, where E has a zero-mean normal distribution with variance equal to σ_e^2, as would be the case if $\breve{\mu}$ were the minimum mean square estimate (MMSE) based on prior observations with additive Gaussian obfuscation. We consider not only the leakage of true data (**X**) but also the leakage of distribution of true data (μ), which is a serious issue.

5.4.1 Without Remapping Technique

If remapping is not employed, the user's intended friend observes the reported data (Y). Thus, the MSE of the application is

$$\mathcal{UD}_{NR}^{(II)} = \mathbb{E}\left[\left(\widetilde{X}_{App} - X\right)^2\right] = \mathbb{E}\left[(Y - X)^2\right] = \sigma_w^2. \tag{5.5}$$

In contrast, the sophisticated adversary uses both $Y = \mu + S + W$ and $\breve{\mu} = \mu + E$ to improve her knowledge not only about the true data (X) but also about the distribution of the true data (μ), (Here, we write $X = \mu + S$, where $S \sim \mathcal{N}(0, \sigma_s^2)$). Thus,

$$\begin{bmatrix} \breve{\mu} \\ \\ Y \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \\ 1 & 1 \end{bmatrix} \begin{bmatrix} \mu \\ \\ S \end{bmatrix} + \begin{bmatrix} E \\ \\ W \end{bmatrix}.$$

Thus, the adversary has $\widetilde{\mu}_{Adv} = \mathbb{E}[\mu|Y, \breve{\mu}]$ and $\widetilde{X}_{Adv} = \mathbb{E}[X|Y, \breve{\mu}]$. In the first step, we should calculate the conditional expectation $\mathbb{E}[X|Y, \breve{\mu}]$ required for the minimum mean square error estimator (MMSE). Note that the MMSE estimate in the case of bivariate Gaussian variables has a nice linear form, which will be called linear minimum mean square error (LMMSE) estimator. Using linear MMSE, S and μ given $\breve{\mu}$ and Y have linear forms as

$$\widetilde{\mu}_{Adv} = a_0 + a_1 Y + a_2 \breve{\mu}, \tag{5.6}$$

s

$$\widetilde{S}_{Adv} = b_0 + b_1 Y + b_2 \breve{\mu}, \tag{5.7}$$

where a_0, a_1, a_2, b_0, b_1, and b_2 are to be determined in order to minimize the MSE.

Note that the linear MMSE should satisfy:

- $\mathbb{E}\left[X - \widetilde{X}_{Adv}\right] = 0$, in other words,
  - $\mathbb{E}[\mu] = \mathbb{E}[\widetilde{\mu}_{Adv}]$.
  - $\mathbb{E}[S] = \mathbb{E}\left[\widetilde{S}_{Adv}\right]$.

- $\mathrm{Cov}\left(X - \widetilde{X}_{Adv}, \breve{\mu}\right) = 0$, in other words,
    - $\mathrm{Cov}\left(\mu, \breve{\mu}\right) = \mathrm{Cov}\left(\widetilde{\mu}_{Adv}, \breve{\mu}\right).$
    - $\mathrm{Cov}\left(S, \breve{\mu}\right) = \mathrm{Cov}\left(\widetilde{S}_{Adv}, \breve{\mu}\right).$
- $\mathrm{Cov}\left(X - \widetilde{X}_{Adv}, Y\right) = 0$, in other words,
    - $\mathrm{Cov}\left(\mu, Y\right) = \mathrm{Cov}\left(\widetilde{\mu}_{Adv}, Y\right).$
    - $\mathrm{Cov}\left(S, Y\right) = \mathrm{Cov}\left(\widetilde{S}_{Adv}, Y\right).$

In order to satisfy the conditions of linear MMSE, a_0, a_1, a_2, b_0, b_1, and b_2 are calculated as

$$
\begin{aligned}
a_0 &= b_0 = 0. \\
a_1 &= \frac{\sigma_\mu^2 \sigma_e^2}{\left(\sigma_\mu^2 + \sigma_e^2\right)\left(\sigma_s^2 + \sigma_w^2\right) + \sigma_e^2 \sigma_\mu^2}. \\
b_1 &= \frac{\sigma_s^2 \left(\sigma_\mu^2 + \sigma_e^2\right)}{\left(\sigma_\mu^2 + \sigma_e^2\right)\left(\sigma_s^2 + \sigma_w^2\right) + \sigma_e^2 \sigma_\mu^2}. \\
a_2 &= \frac{\sigma_\mu^2 \left(\sigma_s^2 + \sigma_w^2\right)}{\left(\sigma_\mu^2 + \sigma_e^2\right)\left(\sigma_s^2 + \sigma_w^2\right) + \sigma_e^2 \sigma_\mu^2}. \\
b_2 &= \frac{-\sigma_s^2 \sigma_\mu^2}{\left(\sigma_\mu^2 + \sigma_e^2\right)\left(\sigma_s^2 + \sigma_w^2\right) + \sigma_e^2 \sigma_\mu^2}.
\end{aligned}
$$

Thus, $\widetilde{\mu}_{Adv} = \mathbb{E}\left[\mu | Y, \breve{\mu}\right]$ is

$$
\begin{aligned}
\widetilde{\mu}_{Adv} = & \frac{\sigma_\mu^2 \sigma_e^2}{\left(\sigma_\mu^2 + \sigma_e^2\right)\left(\sigma_s^2 + \sigma_w^2\right) + \sigma_e^2 \sigma_\mu^2} Y + \\
& \frac{\sigma_\mu^2 \left(\sigma_s^2 + \sigma_w^2\right)}{\left(\sigma_\mu^2 + \sigma_e^2\right)\left(\sigma_s^2 + \sigma_w^2\right) + \sigma_e^2 \sigma_\mu^2} \breve{\mu}.
\end{aligned}
$$

Also, remember $\widetilde{X}_{Adv} = \mathbb{E}\left[X | Y, \breve{\mu}\right] = \widetilde{\mu}_{Adv} + \widetilde{S}_{Adv}$, thus, we have

$$
\begin{aligned}
\widetilde{X}_{Adv} = & \frac{\sigma_s^2 \sigma_\mu^2 + \sigma_s^2 \sigma_e^2 + \sigma_\mu^2 \sigma_e^2}{\left(\sigma_\mu^2 + \sigma_e^2\right)\left(\sigma_s^2 + \sigma_w^2\right) + \sigma_e^2 \sigma_\mu^2} Y + \\
& \frac{\sigma_\mu^2 \sigma_w^2}{\left(\sigma_\mu^2 + \sigma_e^2\right)\left(\sigma_s^2 + \sigma_w^2\right) + \sigma_e^2 \sigma_\mu^2}.
\end{aligned}
$$

Now, the MSE of the adversary about the distribution of true data (μ) is calculated as:

$$\begin{aligned}\grave{\mathcal{P}}_{NR}^{(II)} &= \mathbb{E}\left[(\widetilde{\mu}_{Adv} - \mu)^2\right] \\ &= \frac{\sigma_e^2\sigma_\mu^2\left(\sigma_s^2 + \sigma_w^2\right)}{\left(\sigma_\mu^2 + \sigma_e^2\right)\left(\sigma_s^2 + \sigma_w^2\right) + \sigma_e^2\sigma_\mu^2}.\end{aligned} \tag{5.8}$$

and MSE of the adversary about true data (X) is calculated as:

$$\begin{aligned}\mathcal{P}_{NR}^{(II)} &= \mathbb{E}\left[\left(\widetilde{X}_{Adv} - X\right)^2\right] \\ &= \frac{\sigma_s^2\sigma_w^2}{\sigma_s^2 + \sigma_w^2} + \frac{\sigma_w^4\sigma_e^2\sigma_\mu^2}{\left(\sigma_s^2 + \sigma_w^2\right)\left(\left(\sigma_\mu^2 + \sigma_e^2\right)\left(\sigma_s^2 + \sigma_w^2\right) + \sigma_e^2\sigma_\mu^2\right)}.\end{aligned} \tag{5.9}$$

Extension to m observations: In the next step, we assume the adversary observes m observations of the user, and tries to use all of her observations to make better estimations about both true data ($\mathbf{X}$) and the distribution of true data (μ). Note that she has

- $\breve{\mu} = \mu + E$.
- $Y(k) = \mu + S(K) + W(k)$, for $k \in \{1, 2, \cdots, m\}$.

The adversary should calculate $\widetilde{\mu}_{Adv} = \mathbb{E}\left[\mu | \mathbf{Y}, \breve{\mu}\right]$ and $\widetilde{\mathbf{X}}_{Adv} = \mathbb{E}\left[\mathbf{X} | \mathbf{Y}, \breve{\mu}\right]$.

Using linear MMSE, $S(1)$ and μ given $\breve{\mu}$ and $\mathbf{Y}$ have linear forms as

$$\widetilde{\mu}_{Adv} = a_0 + a_1Y(1) + a_2Y(2) + \cdots + a_mY(m) + a_{m+1}\breve{\mu}, \tag{5.10}$$

and

$$\widetilde{S(1)}_{Adv} = b_0 + b_1Y(1) + b_2Y(2) + \cdots + b_mY(m) + b_{m+1}\breve{\mu}, \tag{5.11}$$

where a_k's and b_k's are to be determined in order to minimize the MSE.

In order to satisfy the conditions of linear MMSE, we have

$$a_0 = b = 0$$

$$a_1 = \frac{\sigma_\mu^2\sigma_e^2}{\left(\sigma_\mu^2+\sigma_e^2\right)\left(\sigma_s^2+\sigma_w^2\right)+m\sigma_e^2\sigma_\mu^2},$$

$$b_1 = \frac{\sigma_s^2\left(\sigma_\mu^2+\sigma_e^2\right)}{\left(\sigma_\mu^2+\sigma_e^2\right)\left(\sigma_s^2+\sigma_w^2\right)+m\sigma_e^2\sigma_\mu^2} + \frac{(m-1)\sigma_s^2\sigma_\mu^2\sigma_e^2}{\left(\sigma_s^2+\sigma_w^2\right)\left(\left(\sigma_\mu^2+\sigma_e^2\right)\left(\sigma_s^2+\sigma_w^2\right)+m\sigma_e^2\sigma_\mu^2\right)}.$$

$$a_k = \frac{\sigma_\mu^2\sigma_e^2}{\left(\sigma_\mu^2+\sigma_e^2\right)\left(\sigma_s^2+\sigma_w^2\right)+m\sigma_e^2\sigma_\mu^2}, \text{ for } k \in \{2,3,\cdots,m\}.$$

$$b_k = \frac{-\sigma_e^2\sigma_\mu^2\sigma_s^2}{\left(\sigma_s^2+\sigma_w^2\right)\left(\left(\sigma_\mu^2+\sigma_e^2\right)\left(\sigma_s^2+\sigma_w^2\right)+m\sigma_e^2\sigma_\mu^2\right)}, \text{ for } k \in \{2,3,\cdots,m\}.$$

$$a_{m+1} = \frac{\sigma_\mu^2\left(\sigma_s^2+\sigma_w^2\right)}{\left(\sigma_\mu^2+\sigma_e^2\right)\left(\sigma_s^2+\sigma_w^2\right)+m\sigma_e^2\sigma_\mu^2}$$

$$b_{m+1} = \frac{-\sigma_s^2\sigma_\mu^2}{\left(\sigma_\mu^2+\sigma_e^2\right)\left(\sigma_s^2+\sigma_w^2\right)+m\sigma_e^2\sigma_\mu^2}.$$

Thus, $\widetilde{\mu}_{Adv} = \mathbb{E}\left[\mu|\mathbf{Y},\breve{\mu}\right]$ can be calculated as

$$\begin{aligned}\widetilde{\mu}_{Adv} &= \sum_{k=1}^{m}\frac{\sigma_\mu^2\sigma_e^2}{\left(\sigma_\mu^2+\sigma_e^2\right)\left(\sigma_s^2+\sigma_w^2\right)+m\sigma_e^2\sigma_\mu^2}Y(k)\\ &+ \frac{\sigma_\mu^2\left(\sigma_s^2+\sigma_w^2\right)}{\left(\sigma_\mu^2+\sigma_e^2\right)\left(\sigma_s^2+\sigma_w^2\right)+m\sigma_e^2\sigma_\mu^2}\breve{\mu}.\end{aligned}$$

Also, remember $\widetilde{X(1)}_{Adv} = \mathbb{E}\left[X(1)|\mathbf{Y},\breve{\mu}\right] = \widetilde{\mu}_{Adv} + \widetilde{S(1)}_{Adv}$, thus, we have

$$\begin{aligned}\widetilde{X(1)}_{Adv} &= \frac{\left(\sigma_s^2\sigma_\mu^2+\sigma_s^2\sigma_e^2+\sigma_\mu^2\sigma_e^2\right)\left(\sigma_s^2+\sigma_w^2\right)+(m-1)\sigma_s^2\sigma_\mu^2\sigma_e^2}{\left(\sigma_s^2+\sigma_w^2\right)\left(\left(\sigma_\mu^2+\sigma_e^2\right)\left(\sigma_s^2+\sigma_w^2\right)+m\sigma_e^2\sigma_\mu^2\right)}Y(1) \qquad (5.12)\\ &+\sum_{k=2}^{m}\frac{\sigma_e^2\sigma_\mu^2\sigma_w^2}{\left(\sigma_s^2+\sigma_w^2\right)\left(\left(\sigma_\mu^2+\sigma_e^2\right)\left(\sigma_s^2+\sigma_w^2\right)+m\sigma_e^2\sigma_\mu^2\right)}Y(k)\\ &+\frac{\sigma_\mu^2\sigma_w^2}{\left(\sigma_\mu^2+\sigma_e^2\right)\left(\sigma_s^2+\sigma_w^2\right)+m\sigma_e^2\sigma_\mu^2}\breve{\mu}.\end{aligned}$$

(5.13)

Now, the MSE of the adversary about the distribution of the true data (μ) can be calculated as

$$\begin{aligned}\grave{\mathcal{P}}_{NR}^{(II)} &= \mathbb{E}\left[(\widetilde{\mu}_{Adv} - \mu)^2\right] \\ &= \frac{\sigma_e^2\sigma_\mu^2\left(\sigma_s^2+\sigma_w^2\right)}{\left(\sigma_s^2+\sigma_w^2\right)\left(\sigma_\mu^2+\sigma_e^2\right)+m\sigma_e^2\sigma_\mu^2},\end{aligned} \tag{5.14}$$

and the MSE of the adversary about user' true data at time k, $X(K)$, can be calculated as

$$\begin{aligned}&\mathcal{P}_{NR}^{(II)} = \mathbb{E}\left[\left(\widetilde{X(k)}_{Adv} - X(k)\right)^2\right] \\ &= \frac{\sigma_s^2\sigma_w^2}{\sigma_s^2+\sigma_w^2} + \frac{\sigma_w^4\sigma_e^2\sigma_\mu^2}{\left(\sigma_s^2+\sigma_w^2\right)\left(\left(\sigma_s^2+\sigma_w^2\right)\left(\sigma_\mu^2+\sigma_e^2\right)+m\sigma_e^2\sigma_\mu^2\right)}.\end{aligned} \tag{5.15}$$

5.4.2 With Remapping Technique

If the remapping technique is employed, our friend observes the remapped data, so, the MSE of the application can be quantified as:

$$\mathcal{UD}_R^{(II)} = \mathbb{E}\left[\left(\widetilde{X}_{App} - X\right)^2\right] = \mathbb{E}\left[(Y_R - X)^2\right] = \frac{\sigma_s^2\sigma_w^2}{\sigma_s^2+\sigma_w^2}. \tag{5.16}$$

However, the adversary observes not only Y_R, but also $\breve{\mu}$, and uses both of them to estimate $\widetilde{\mu}_{Adv}$ and $\widetilde{X}_{Adv}$. In other words,

$$\begin{bmatrix} \breve{\mu} \\ \\ Y_R \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \\ 1 & \frac{\sigma_s^2}{\sigma_s^2+\sigma_w^2} \end{bmatrix} \begin{bmatrix} \mu \\ \\ S \end{bmatrix} + \begin{bmatrix} E \\ \\ \frac{\sigma_s^2}{\sigma_s^2+\sigma_w^2} W \end{bmatrix}.$$

Using linear MMSE, S and μ given $\breve{\mu}$ and Y have linear forms as

$$\widetilde{\mu}_{Adv} = a_0 + a_1 Y_R + a_2 \breve{\mu}, \tag{5.17}$$

and

$$\widetilde{S}_{Adv} = b_0 + b_1 Y_R + b_2 \breve{\mu}, \tag{5.18}$$

where a_0, a_1, a_2, b_0, b_1, and b_2 are to be determined in order to minimize the MSE.

Note the linear MMSE should satisfy:

- $\mathbb{E}\left[X - \widetilde{X}_{Adv}\right] = 0$, in other words,
  - $\mathbb{E}[\mu] = \mathbb{E}[\widetilde{\mu}_{Adv}]$.
  - $\mathbb{E}[S] = \mathbb{E}\left[\widetilde{S}_{Adv}\right]$.
- $\mathrm{Cov}\left(X - \widetilde{X}_{Adv}, \breve{\mu}\right) = 0$, in other words,
  - $\mathrm{Cov}(\mu, \breve{\mu}) = \mathrm{Cov}(\widetilde{\mu}_{Adv}, \breve{\mu})$.
  - $\mathrm{Cov}(S, \breve{\mu}) = \mathrm{Cov}\left(\widetilde{S}_{Adv}, \breve{\mu}\right)$.
- $\mathrm{Cov}\left(X - \widetilde{X}_{Adv}, Y_R\right) = 0$, in other words,
  - $\mathrm{Cov}(\mu, Y_R) = \mathrm{Cov}(\widetilde{\mu}_{Adv}, Y_R)$.
  - $\mathrm{Cov}(S, Y_R) = \mathrm{Cov}\left(\widetilde{S}_{Adv}, Y_R\right)$.

In order to satisfy the conditions of linear MMSE, a_0, a_1, a_2, b_0, b_1, and b_2 are calculated as

$$a_0 = b_0 = 0,$$

$$a_1 = \frac{\sigma_e^2 \sigma_\mu^2 \left(\sigma_s^2 + \sigma_w^2\right)}{\sigma_s^4 \left(\sigma_\mu^2 + \sigma_e^2\right) + \sigma_e^2 \sigma_\mu^2 \left(\sigma_s^2 + \sigma_w^2\right)}$$

$$b_1 = \frac{\sigma_s^4 \left(\sigma_\mu^2 + \sigma_e^2\right)}{\sigma_s^4 \left(\sigma_\mu^2 + \sigma_e^2\right) + \sigma_e^2 \sigma_\mu^2 \left(\sigma_s^2 + \sigma_w^2\right)}$$

$$a_2 = \frac{\sigma_s^4 \sigma_\mu^2}{\sigma_s^4 \left(\sigma_\mu^2 + \sigma_e^2\right) + \sigma_e^2 \sigma_\mu^2 \left(\sigma_s^2 + \sigma_w^2\right)}$$

$$b_2 = \frac{-\sigma_s^4 \sigma_\mu^2}{\sigma_s^4 \left(\sigma_\mu^2 + \sigma_e^2\right) + \sigma_e^2 \sigma_\mu^2 \left(\sigma_s^2 + \sigma_w^2\right)}$$

Thus, $\widetilde{\mu}_{Adv} = \mathbb{E}\left[\mu | Y_R, \breve{\mu}\right]$ can be calculated as

$$\begin{aligned}\widetilde{\mu}_{Adv} = & \frac{\sigma_\mu^2 \sigma_m^2 \left(\sigma_s^2 + \sigma_w^2\right)}{\sigma_s^4 \left(\sigma_\mu^2 + \sigma_e^2\right) + \sigma_e^2 \sigma_\mu^2 \left(\sigma_s^2 + \sigma_w^2\right)} Y_R \\ & + \frac{\sigma_s^4 \sigma_\mu^2}{\sigma_s^4 \left(\sigma_\mu^2 + \sigma_e^2\right) + \sigma_e^2 \sigma_\mu^2 \left(\sigma_s^2 + \sigma_w^2\right)} \breve{\mu}.\end{aligned}$$

Remember $\widetilde{X}_{Adv} = \mathbb{E}\left[X | Y_R, \breve{\mu}\right] = \widetilde{\mu}_{Adv} + \widetilde{S}_{Adv}$, so we have

$$\widetilde{X}_{Adv} = Y_R.$$

Now, the MSE of the adversary about the distribution of true data (μ) can be calculated as

$$\begin{aligned}\grave{\mathcal{P}}_{NR}^{(II)} & = \mathbb{E}\left[\left(\widetilde{\mu}_{Adv} - \mu\right)^2\right] \\ & = \frac{\sigma_s^4 \sigma_e^2 \sigma_\mu^2}{\sigma_s^4 \left(\sigma_\mu^2 + \sigma_e^2\right) + \sigma_e^2 \sigma_\mu^2 \left(\sigma_s^2 + \sigma_w^2\right)},\end{aligned} \tag{5.19}$$

and the MSE of the adversary about true data (X) can be calculated as

$$\begin{aligned}\mathcal{P}_R^{(II)} = & \mathbb{E}\left[\left(\widetilde{X}_{Adv} - X\right)^2\right] \\ = & \frac{\sigma_s^2 \sigma_w^2}{\sigma_s^2 + \sigma_w^2}.\end{aligned} \tag{5.20}$$

Extension to m observations: Now, we assume the adversary observes m observations of the user, so, she has

- $\breve{\mu} = \mu + E$.
- $Y_R(k) = \mu + \frac{\sigma_s^2}{\sigma_s^2 + \sigma_w^2} S(k) + \frac{\sigma_s^2}{\sigma_s^2 + \sigma_w^2} W(k)$, for $k \in \{1, 2, \cdots, m\}$.

The adversary should calculates $\widetilde{\mu}_{Adv} = \mathbb{E}\left[\mu|\mathbf{Y}_R, \breve{\mu}\right]$ and $\widetilde{\mathbf{X}}_{Adv} = \mathbb{E}\left[\mathbf{X}|\mathbf{Y}_R, \breve{\mu}\right]$. Using linear MMSE, $S(1)$ and μ given $\breve{\mu}$ and $\mathbf{Y}_R$ have linear forms as

$$\widetilde{\mu}_{Adv} = a_0 + a_1 Y_R(1) + a_2 Y_R(2) + \cdots + a_m Y_R(m) + a_{m+1}\breve{\mu}, \tag{5.21}$$

and

$$\widetilde{S(1)}_{Adv} = b_0 + b_1 Y_R(1) + b_2 Y_R(2) + \cdots + b_m Y_R(m) + b_{m+1}\breve{\mu}, \tag{5.22}$$

where a_k's and b_k's are to be determined in order to minimize the MSE. In order to satisfy the conditions of linear MMSE, we have

$$a_0 = b_0 = 0$$

$$a_1 = \frac{\sigma_\mu^2\sigma_e^2\left(\sigma_s^2+\sigma_w^2\right)}{\sigma_s^4\left(\sigma_\mu^2+\sigma_e^2\right)+m\sigma_e^2\sigma_\mu^2\left(\sigma_s^2+\sigma_w^2\right)}.$$

$$b_1 = \frac{\sigma_s^4\left(\sigma_\mu^2+\sigma_e^2\right)}{\sigma_s^4\left(\sigma_\mu^2+\sigma_e^2\right)+m\sigma_e^2\sigma_\mu^2\left(\sigma_s^2+\sigma_w^2\right)} + \frac{(m-1)\,\sigma_e^2\sigma_s^2\sigma_\mu^2\left(\sigma_s^2+\sigma_w^2\right)}{\sigma_s^4\left(\sigma_\mu^2+\sigma_e^2\right)+m\sigma_e^2\sigma_\mu^2\left(\sigma_s^2+\sigma_w^2\right)}.$$

$$a_k = \frac{\sigma_\mu^2\sigma_e^2\left(\sigma_s^2+\sigma_w^2\right)}{\sigma_s^4\left(\sigma_\mu^2+\sigma_e^2\right)+m\sigma_e^2\sigma_\mu^2\left(\sigma_s^2+\sigma_w^2\right)}, \text{ for } k \in \{2,3,\cdots,m\}.$$

$$b_k = \frac{-\sigma_\mu^2\sigma_e^2\left(\sigma_s^2+\sigma_w^2\right)}{\sigma_s^4\left(\sigma_\mu^2+\sigma_e^2\right)+m\sigma_e^2\sigma_\mu^2\left(\sigma_s^2+\sigma_w^2\right)},, \text{ for } k \in \{2,3,\cdots,m\}.$$

$$a_{m+1} = \frac{\sigma_s^4\sigma_\mu^2}{\sigma_s^4\left(\sigma_\mu^2+\sigma_e^2\right)+m\sigma_e^2\sigma_\mu^2\left(\sigma_s^2+\sigma_w^2\right)}.$$

$$b_{m+1} = \frac{-\sigma_s^4\sigma_\mu^2}{\sigma_s^4\left(\sigma_\mu^2+\sigma_e^2\right)+m\sigma_e^2\sigma_\mu^2\left(\sigma_s^2+\sigma_w^2\right)}.$$

Thus, $\widetilde{\mu}_{Adv} = \mathbb{E}\left[\mu|\mathbf{Y}_R, \breve{\mu}\right]$ can be calculated as

$$\begin{aligned}\widetilde{\mu}_{Adv} = \sum_{k=1}^{m} &\frac{\sigma_\mu^2\sigma_e^2\left(\sigma_s^2+\sigma_w^2\right)}{\sigma_s^4\left(\sigma_\mu^2+\sigma_e^2\right)+m\sigma_e^2\sigma_\mu^2\left(\sigma_s^2+\sigma_w^2\right)}Y_R(m)\\ &+ \frac{\sigma_s^4\sigma_\mu^2}{\sigma_s^4\left(\sigma_\mu^2+\sigma_e^2\right)+m\sigma_e^2\sigma_\mu^2\left(\sigma_s^2+\sigma_w^2\right)}\breve{\mu}.\end{aligned}$$

and $\widetilde{X(1)}_{Adv} = \mathbb{E}\left[X(1)|\mathbf{Y}_R, \breve{\mu}\right] = \widetilde{\mu}_{Adv} + \widetilde{S(1)}_{Adv}$, so, we can conclude

$$\widetilde{X(1)}_{Adv} = Y_R(1),$$

As a result, the MSE of the adversary about the distribution of the true data (μ) can be calculated as

$$\begin{aligned}\grave{\mathcal{P}}_R^{(II)} &= \mathbb{E}\left[\left(\widetilde{\mu}_{Adv} - \mu\right)^2\right] \\ &= \frac{\sigma_e^2 \sigma_\mu^2 \sigma_s^4}{\sigma_s^4\left(\sigma_\mu^2 + \sigma_e^2\right) + m\sigma_e^2\sigma_\mu^2\left(\sigma_s^2 + \sigma_w^2\right)},\end{aligned} \tag{5.23}$$

and the MSE of the adversary about true data at time k, $X(k)$, can be calculated as

$$\begin{aligned}\mathcal{P}_R^{(II)} =& \mathbb{E}\left[\left(\widetilde{X(k)}_{Adv} - X(k)\right)^2\right] \\ =& \frac{\sigma_s^2\sigma_w^2}{\sigma_s^2 + \sigma_w^2}.\end{aligned} \tag{5.24}$$

5.4.3 Discussion: Leakage of the Statistical Model

By (5.19) and (5.23), we can conclude that increasing the obfuscation noise somewhat surprisingly increases the leakage about the distribution of the true data (μ) when remapping is employed. Note that $\mathbf{Y}_R = \mathbb{E}\left[\mathbf{X}|\mathbf{Y}, \breve{\mu}\right]$ depends on two parameters: 1) $\breve{\mu} = \mu + E$ and 2) $\mathbf{Y} = \mathbf{X} + \mathbf{W}$; thus, if we increase the obfuscation noise by increasing σ_w^2, $\mathbf{Y}_R$ relies less on $\mathbf{Y}$ and more on $\breve{\mu}$. Now in the extreme case, where σ_w^2 goes to infinity, the observed data ($\mathbf{Y}$) is useless and, as a result, $\mathbf{Y}_R = \mathbb{E}\left[\mathbf{X}|\mathbf{Y}, \breve{\mu}\right] = \mu$. Hence, remapping leaks complete information about the statistical model (μ) as σ_w^2 goes to infinity.

5.5 Randomized Remapping

As derived in Section 5.4, the remapping technique can leak a lot of information about the distribution of the true data (μ) if the adversary does not have the perfect prior about the user. Here, we introduce a new technique called randomized remapping to improve privacy. This technique provides a trade-off between the leakage of the distribution of the true data (μ) and the leakage of true data ($\mathbf{X}$). In the randomized remapping, we have an unfair coin where the probability of a head is equal to p_H. For each data point, we toss the coin and if a head is observed, the remapped data (Y_R) is released, and if a tail is observed, the noisy version of data (Y) is released. As a result,

$$Z = \begin{cases} Y_R, & \text{with probability } p_H, \\ Y, & \text{with probability of } 1 - p_H, \end{cases}$$

Here, user's friend observes Z, thus, the MSE of the application can be calculated as,

$$\mathcal{UD}_{Rand}^{(III)} = \mathbb{E}\left[(Z - X)^2\right] = p_H \frac{\sigma_w^2}{\sigma_w^2 + \sigma_s^2} + (1 - p_H)\,\sigma_w^2. \tag{5.25}$$

However, the adversary observes both Z and $\check{\mu} = \mu + E$ to estimate the true data (X) and distribution of the true data (μ). We can calculate $\grave{\mathcal{P}}_{Rand}^{(III)}$ which indicates the MSE of the adversary about the distribution of true data (μ) as:

$$\grave{\mathcal{P}}_{Rand}^{(III)} = \mathbb{E}\left[(\widetilde{\mu}_{Adv} - \mu)^2\right]. \tag{5.26}$$

Figure 5.3 shows the MSE of the adversary about the statistical model ($\grave{\mathcal{P}}_{Rand}^{(III)}$) versus the MSE of the intended application/friend ($\mathcal{UD}_{Rand}^{(III)}$).

We can also calculate $\mathcal{P}_{Rand}^{(III)}$ which indicates the MSE of the adversary about the true data (μ) as:

$$\mathcal{P}_{Rand}^{(III)} = \mathbb{E}\left[\left(\widetilde{X}_{Adv} - \mu\right)^2\right]. \tag{5.27}$$

Figure 5.4 shows the MSE of the adversary ($\mathcal{P}_{Rand}^{(III)}$) versus the MSE of the intended application/friend ($\mathcal{UD}_{Rand}^{(III)}$).

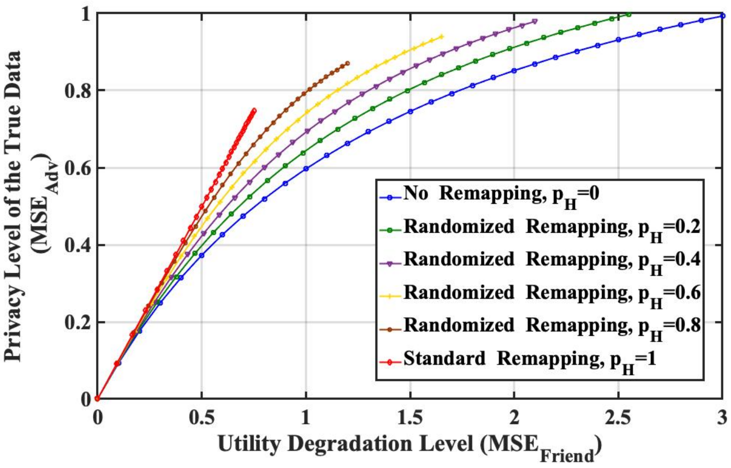


Figure 5.3: The MSE of the adversary about the statistical model (μ) versus the MSE of the application for three cases. Case 1: remapping technique is not employed ($p_H = 0$), Case 2: a randomized remapping technique is employed with $p_H = 0.2$, 0.4, 0.6, and 0.8, and Case 3: standard remapping [12] is employed ($p_H = 1$). Here, we assume $\sigma_\mu^2 = \sigma_e^2 = \sigma_s^2 = 1$ and σ_w^2 is swept from 0 to 1 with steps of 0.1.

From Figures 5.3 and 5.4, we can conclude that the standard remapping leaks a lot of information about the statistical model, while providing the best privacy level about the user' true data. Here, the randomized remapping provides a much better trade-off compared to standard remapping. The value of p_H is a design parameter, so, based on the application requirements and privacy requirements, the appropriate amount of p_H should be chosen.

5.6 Appendix

Here, the mutual information is employed as a metric to quantify both utility and privacy. In this paper, ”$\mathcal{U}$” denotes the mutual information between the true data and signal receive by the intended application/friend; this quantifies the system's utility. Likewise, ”$\mathcal{L}$” denotes the mutual information between the true data and the adversary's observations; this quantifies the information leakage. Note that the level of privacy can be quantified as $\mathbb{H}(X|Y) = \mathbb{H}(X) - \mathbb{I}(X;Y)$, where $\mathbb{H}(.)$ is the entropy and $\mathbb{I}(.)$ is the mutual information.

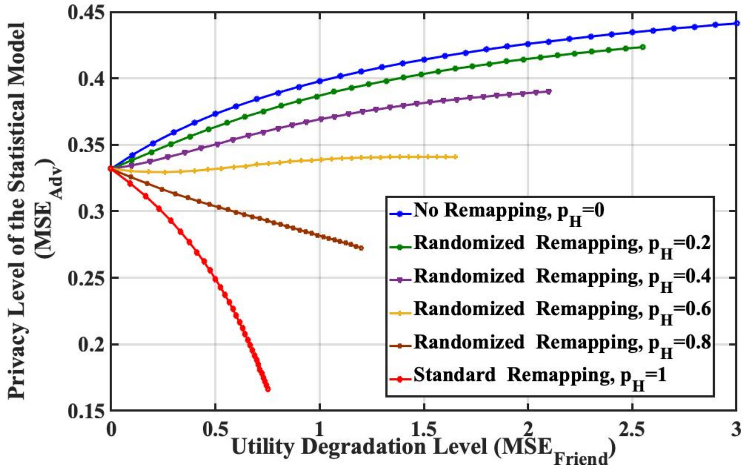


Figure 5.4: The MSE of the adversary about the user' true data (μ) versus the MSE of the application for three cases. Case 1: remapping technique is not employed ($p_H = 0$), Case 2: a randomized remapping technique is employed with $p_H = 0.2$, 0.4, 0.6, and 0.8, and Case 3: standard remapping [12] is employed ($p_H = 1$). Here, we assume $\sigma_\mu^2 = \sigma_e^2 = \sigma_s^2 = 1$ and σ_w^2 is swept from 0 to 1 with steps of 0.1.

Table 5.1: Results of case 1: Perfect knowledge of the adversary.

	Utility	Leakage of true data
Without Remapping	$0.5 \ln \left(\frac{\sigma_w^2 + \sigma_s^2 + \sigma_\mu^2}{\sigma_w^2} \right)$	$0.5 \ln \left(\frac{\sigma_w^2 + \sigma_s^2}{\sigma_w^2} \right)$
With Remapping	$0.5 \ln \left(\frac{\sigma_w^2 + \sigma_s^2 + \sigma_\mu^2}{\sigma_w^2} + \frac{\sigma_\mu^2}{\sigma_s^2} \right)$	$0.5 \ln \left(\frac{\sigma_w^2 + \sigma_s^2}{\sigma_w^2} \right)$

Here, our goal is to minimize the information leakage to maximize the level of privacy at the highest possible utility.

5.6.1 Case 1: Perfect Knowledge of the Adversary

In this section, we assume the adversary knows the exact value of the mean (μ). The results for the case the remapping technique is employed and the case remapping technique is not employed are shown in Table 5.1.

Table 5.2: Utility for case 2: Imperfect knowledge of the adversary, one observation.

	Utility
Without Remapping	$0.5 \ln \left(\frac{\sigma_w^2 + \sigma_s^2 + \sigma_\mu^2}{\sigma_w^2} \right)$
With Remapping	$0.5 \ln \left(\frac{\sigma_w^2 + \sigma_s^2 + \sigma_\mu^2}{\sigma_w^2} + \frac{\sigma_\mu^2}{\sigma_s^2} \right)$

Since the intended friend/application is oblivious to the prior statistical knowledge about the user behavior, we always have $\mathcal{L} \leq \mathcal{U}$. As you can observed in Table 5.1, we can conclude the remapping technique provides the best utility among techniques satisfying the same level of privacy in the case of perfect knowledge of the adversary [12].

5.6.2 Case 2: Imperfect Knowledge of the Adversary

Here, we assume the adversary has a noisy version of the prior information, as might be obtained from a learning set of limited length. Specifically, the adversary has $\breve{\mu} = \mu + E$, where E has a zero-mean normal distribution with variance equal to σ_e^2, as would be the case if $\breve{\mu}$ were the minimum mean square estimate (MMSE) based on prior observations with additive Gaussian obfuscation. We consider not only the leakage of true data ($\mathbf{X}$) but also the leakage of distribution of true data (μ), which is a serious issue. The results for the case the remapping technique is employed and the case remapping technique is not employed are shown in Tables 5.2, 5.3, and 5.4.

Extension to m observations: Next, we assume the adversary observes m samples from the user, and tries to use all of her observations to make better estimations about both the true data ($\mathbf{X}$) and the distribution of the true data (μ). The results for the case the remapping technique is employed and the case remapping technique is not employed are shown in Tables 5.5 and 5.6.

Table 5.3: Leakage of true data for case 2: Imperfect knowledge of the adversary, one observation.

	Leakage of true data
Without Remapping	$0.5\ln\left(\frac{\sigma_s^2+\sigma_w^2}{\sigma_w^2}+\frac{\sigma_e^2\sigma_\mu^2}{\sigma_w^2(\sigma_e^2+\sigma_\mu^2)}\right)$
With Remapping	$0.5\ln\left(\frac{\sigma_s^2+\sigma_w^2}{\sigma_w^2}+\frac{\sigma_e^2\sigma_\mu^2(\sigma_s^2+\sigma_w^2)}{\sigma_s^2\sigma_w^2(\sigma_e^2+\sigma_\mu^2)}\right)$

Table 5.4: Leakage of the statistical model for case 2: Imperfect knowledge of the adversary, one observation.

	Leakage of the statistical model
Without Remapping	$0.5\ln\left(1+\frac{\sigma_e^2\sigma_\mu^2}{(\sigma_s^2+\sigma_w^2)(\sigma_e^2+\sigma_\mu^2)}\right)$
With Remapping	$0.5\ln\left(1+\frac{\sigma_e^2\sigma_\mu^2(\sigma_s^2+\sigma_w^2)}{\sigma_s^4(\sigma_e^2+\sigma_\mu^2)}\right)$

Table 5.5: Leakage of true data for case 2: Imperfect knowledge of the adversary, *m* observations.

	Leakage of true data
Without Remapping	$0.5\ln\left(\frac{\sigma_s^2+\sigma_w^2}{\sigma_w^2}+\frac{\sigma_e^2\sigma_\mu^2}{\sigma_w^2(\sigma_e^2+\sigma_\mu^2)}+\frac{(m-1)\sigma_e^4\sigma_\mu^4/(\sigma_e^2+\sigma_\mu^2)}{(\sigma_s^2+\sigma_w^2)(\sigma_s^2\sigma_e^2+\sigma_s^2\sigma_\mu^2+\sigma_e^2\sigma_\mu^2)+(m-1)\sigma_s^2\sigma_e^2\sigma_\mu^2}\right)$
With Remapping	$0.5\ln\left(\frac{\sigma_s^2+\sigma_w^2}{\sigma_w^2}+\frac{\sigma_e^2\sigma_\mu^2(\sigma_s^2+\sigma_w^2)}{\sigma_s^2\sigma_w^2(\sigma_e^2+\sigma_\mu^2)}\right)$

Table 5.6: Leakage of the statistical model for case 2: Imperfect knowledge of the adversary, m observations.

	Leakage of the statistical model
Without Remapping	$0.5\ln\left(1+\frac{m\sigma_e^2\sigma_\mu^2}{(\sigma_s^2+\sigma_w^2)(\sigma_e^2+\sigma_\mu^2)}\right)$
With Remapping	$0.5\ln\left(1+\frac{m\sigma_e^2\sigma_\mu^2(\sigma_s^2+\sigma_w^2)}{\sigma_s^4(\sigma_e^2+\sigma_\mu^2)}\right)$

5.6.3 Randomized Remapping

In the randomized remapping, we have an unfair coin where the probability of a head is equal to p_H. For each data point, we toss the coin and if a head is observed, the remapped data (Y_R) is released, and if a tail is observed, the noisy version of data (Y) is released. As a result,

$$Z = \begin{cases} Y_R, & \text{with probability } p_H, \\ Y, & \text{with probability of } 1 - p_H, \end{cases}$$

Here, user's friend observes Z, thus, the utility level can be calculated as:

$$\mathcal{U}_{Rand}^{(III)} = \mathbb{I}(X;Z) = 0.5p_H \ln\left(\frac{\sigma_w^2+\sigma_s^2+\sigma_\mu^2}{\sigma_w^2} + \frac{\sigma_\mu^2}{\sigma_s^2}\right) + 0.5\,(1-p_H)\ln\left(\frac{\sigma_w^2+\sigma_s^2+\sigma_\mu^2}{\sigma_w^2}\right)$$

However, the adversary observes both Z and $\breve{\mu} = \mu + E$ to estimate the true data (X) and distribution of the true data (μ). We can calculate $\grave{\mathcal{L}}_{Rand}^{(III)}$ which indicates the leakage of the statistical model (μ) as:

$$\grave{\mathcal{L}}_{Rand}^{(III)} = \mathbb{I}(\mu; Z|\breve{\mu})\,. \tag{5.28}$$

Figure 5.5 shows the leakage of the statistical model ($\grave{\mathcal{L}}_{Rand}^{(III)}$) versus the level of the system's utility ($\mathcal{U}_{Rand}^{(III)}$). A key point here is that randomized remapping provides a much better trade-off compared to standard remapping.

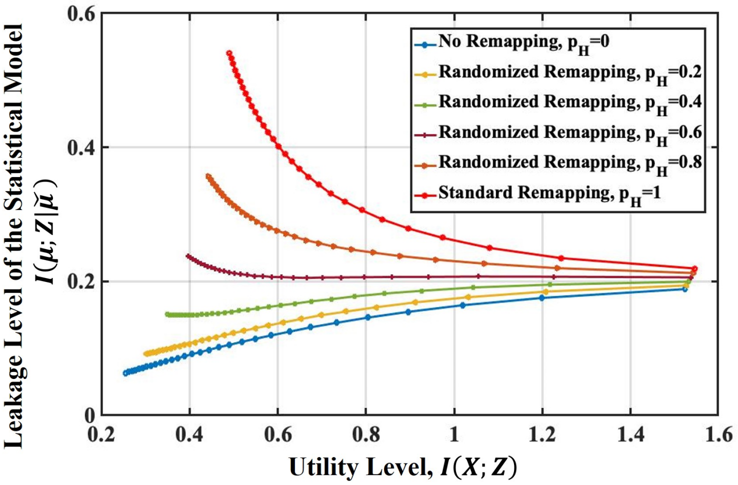


Figure 5.5: The leakage of the statistical model ($\grave{\mathcal{L}}_{Rand}^{(III)}$) versus the level of system's utility ($\mathcal{U}_{Rand}^{(III)}$) for three cases. Case 1: remapping technique is not employed ($p_H = 0$), Case 2: a randomized remapping technique is employed with $p_H = 0.2$, 0.4, 0.6, and 0.8, and Case 3: standard remapping [12] is employed ($p_H = 1$). Here, we assume $\sigma_\mu^2 = \sigma_e^2 = \sigma_s^2 = 1$ and σ_w^2 is swept from 0 to 1 with steps of 0.1.

CHAPTER 6
CONCLUSION

The Internet of Things (IoT) enables users to share and access information on a large scale and provides many benefits to individuals (e.g., smart homes, healthcare) and industries (e.g., digital tracking, data collection, disaster management). However, such benefits are provided by tuning the system to user characteristics based on potentially sensitive information about their activities. Thus, the use of IoT comes with a significant threat to users' privacy: leakage of sensitive information.

Two main privacy-preserving techniques are anonymization and obfuscation, where the former is hiding the mapping between data and the users by replacing the identification fields of users with pseudonyms, and the latter is perturbing the user data such that the adversary observes false but plausible data. Although these methods have been addressed widely, statistical inference methods can be applied to them to break the privacy of the users. Furthermore, achieving privacy using these methods comes with a cost: reducing the utility of the system for the users. Hence, it is crucial to consider the trade-off between privacy and utility when employing privacy-preserving techniques, and to seek to achieve privacy with minimal loss of functionality and usability. Despite the growing interest in IoT privacy, previous works do not offer theoretical guarantees on the trade-off between privacy and utility. In this dissertation, we took a foundational approach to understand the theoretical limits.

Firstly, in Chapter 2, we have considered both obfuscation and anonymization techniques to achieve privacy. The privacy level of the users depends on both $m(n)$ (number of observations per user by the adversary for a fixed anonymization mapping) and a_n (noise level). That is, larger $m(n)$ and smaller a_n indicate weaker privacy. We characterized the limits of privacy in the entire $m(n) - a_n$ plane for the i.i.d. case; that is, we obtained the exact values of the thresholds for $m(n)$ and a_n required for privacy to be maintained. We showed that if $m(n)$ is fewer than $O\left(n^{\frac{2}{r-1}}\right)$, or a_n is larger than $\Omega\left(n^{-\frac{1}{r-1}}\right)$, users have perfect privacy. On the other hand, if neither of these two conditions is satisfied, users have no privacy. For the case where the users' patterns are modeled by Markov chains, we obtained a no-privacy region in the $m(n) - a_n$ plane. Note that in this work we obtained the requirements on anonymization and obfuscation for "perfect" user privacy when traces are independent between users.

Secondly, in Chapter 3, we considered the discrete case, in particular, when the observation sequences are binary sequences, and we focus on the non-asymptotic case where users' data samples are i.i.d.. Then we analyzed the ability of a strong adversary, who knows the prior distribution of users' behavior, to correctly identify users' data samples as a function of the rate of anonymization and degree of obfuscation. We obtained the exact expression for two cases: case 1) only the anonymization technique is used to achieve privacy; case 2) both anonymization and obfuscation techniques are used to achieve privacy. We have shown that the level of privacy of the users depends on three factors: Number of users (n), number of observations per user (m), and noise level (a). We also provide numerical and simulation results for the correct probability in identifying a given user with different parameter settings to investigate the degree to which privacy is protected for various values of n, m, and a. The results were then used to answer a compelling question left open in Chapter 2: can the two techniques could be used productively together in the finite case? In contrast to what previous asymptotic results suggest, we find that the two techniques can be used in conjunction to provide privacy when neither is sufficient by itself.

Thirdly, in Chapter 4, we assumed users have correlated data traces, as relationships between users establish dependence in their behavior. Then, we demonstrated that such dependency degrades the privacy of PPMs, as the anonymization employed must be significantly increased to preserve perfect privacy, and often no degree of independent obfuscation of the traces can be effective. We have also presented preliminary results on dependent obfuscation to improve users' privacy.

Finally, in Chapter 5, we have provided an information-theoretic investigation of the technique of "remapping" which has been introduced in the privacy literature to improve the utility of a naive intended recipient while maintaining the same level of privacy against a sophisticated adversary, in particular one with a prior distribution of the user's data. We first formulated and analyzed remapping under the standard assumption of *perfect* knowledge of the prior at the adversary. Then, we showed that if the adversary has *imperfect* knowledge of the statistics of the user data, the proposed remapping technique introduces leakage about not only the true data but also the user's statistical model. Finally, we proposed a new method termed "randomized remapping" which makes it difficult for the adversary to improve their statistical model at a given utility, thus providing a better utility-privacy trade-off than standard remapping. Since the work here was done under a Gaussian model to facilitate analysis, future research will consider an extension of the analysis and countermeasures to more general models.

Future research in this area needs to characterize the exact privacy/no-privacy regions when the underlying statistical model for users' data are not known. Moreover, for the case, we might not have any clue on what patterns the adversaries obtain. It is also important to consider different ways to obfuscate users' data sets and study the utility-privacy trade-offs for different types of obfuscation techniques. In addition, since the work in Chapter 5 was done under a Gaussian model to facilitate analysis, future research will consider an extension of the analysis and countermeasures to more general models.

BIBLIOGRAPHY

[1] Abbe, Emmanuel. Community detection and stochastic block models: recent developments. *The Journal of Machine Learning Research 18*, 1 (2017), 6446–6531.

[2] Abbe, Emmanuel, and Sandon, Colin. Community detection in general stochastic block models: Fundamental limits and efficient algorithms for recovery. pp. 670–688.

[3] Al Alkeem, Ebrahim, Yeun, Chan Yeob, and Zemerly, M Jamal. Security and privacy framework for ubiquitous healthcare IoT devices. In *Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for* (2015), IEEE, pp. 70–75.

[4] Al-Dhubhani, Raed, and Cazalas, Jonathan. Correlation analysis for geo-indistinguishability based continuous lbs queries. In *2nd International Conference on Anti-Cyber Crimes (ICACC)* (Abha, Saudi Arabia, 2017), IEEE.

[5] Apthorpe, Noah, Reisman, Dillon, and Feamster, Nick. A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. In *Workshop on Data and Algorithmic Transparency* (New York, NY, USA, 2016).

[6] Ardagna, Claudio Agostino, Cremonini, Marco, Damiani, Ernesto, di Vimercati, Sabrina De Capitani, and Samarati, Pierangela. Location privacy protection through obfuscation-based techniques. In *DBSec* (2007).

[7] Babai, László, Erdo"s, Paul, and Selkow, Stanley M. Random graph isomorphism. *SIAM Journal on Computing 9*, 3 (1977), 628–635.

[8] Beresford, Alastair R, and Stajano, Frank. Location privacy in pervasive computing. *IEEE Pervasive computing*, 1 (2003), 46–55.

[9] Bollobás, Béla. Random graphs. Cambridge Studies in Advanced Mathematics.

[10] Bordenabe, Nicolás E, Chatzikokolakis, Konstantinos, and Palamidessi, Catuscia. Optimal geo-indistinguishable mechanisms for location privacy. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (2014), ACM, pp. 251–262.

[11] Calmon, Flavio P, Makhdoumi, Ali, and Médard, Muriel. Fundamental limits of perfect privacy. In *Information Theory (ISIT), 2015 IEEE International Symposium on* (2015), IEEE, pp. 1796–1800.

[12] Chatzikokolakis, K., ElSalamouny, E., and Palamidessi, C. Efficient utility improvement for location privacy. *Proceedings on Privacy Enhancing Technologie 2017*, 4 (2017), 210–231.

[13] Chen, Xu, Chen, Tsung-Yi, and Guo, Dongning. Capacity of gaussian many-access channels. *IEEE Transactions on Information Theory 63*, 6 (2017), 3516–3539.

[14] Chen, Xu, and Guo, Dongning. Many-access channels: The gaussian case with random user activities. In *2014 IEEE International Symposium on Information Theory* (2014), IEEE, pp. 3127–3131.

[15] Chow, Chi-Yin, Mokbel, Mohamed F, and Liu, Xuan. Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments. *GeoInformatica 15*, 2 (2011), 351–380.

[16] Chow, Richard, and Golle, Philippe. Faking contextual data for fun, profit, and privacy. In *Proceedings of the 8th ACM workshop on Privacy in the electronic society* (2009), ACM, pp. 105–108.

[17] Corneil, Derek G., and Kirkpatrick, David G. A theoretical analysis of various heuristics for the graph isomorphism problem. *SIAM Journal on Computing 9*, 2 (1980), 281–297.

[18] Corser, George P, Fu, Huirong, and Banihani, Abdelnasser. Evaluating location privacy in vehicular communications and applications. *IEEE Transactions on Intelligent Transportation Systems 17*, 9 (2016), 2658–2667.

[19] Csiszár, Imre. Almost independence and secrecy capacity. *Problemy Peredachi Informatsii 32*, 1 (1996), 48–57.

[20] Cullina, Daniel, and Kiyavash, Negar. Improved achievability and converse bounds for erdos-renyi graph matching. In *SIGMETRICS* (2016).

[21] Cullina, Daniel, and Kiyavash, Negar. Exact alignment recovery for correlated erdos renyi graphs. *CoRR abs/1711.06783* (2017).

[22] Cullina, Daniel, Mittal, Prateek, and Kiyavash, Negar. Fundamental limits of database alignment. *CoRR abs/1805.03829* (2018).

[23] Cullina, Daniel, Singhal, Kushagra, Kiyavash, Negar, and Mittal, Prateek. On the simultaneous preservation of privacy and community structure in anonymized networks. *CoRR abs/1603.08028* (2016).

[24] Czajka, Tomek, and Pandurangan, Gopal. Improved random graph isomorphism. *J. Discrete Algorithms 6* (2008), 85–92.

[25] Dai, Osman Emre, Cullina, Daniel, and Kiyavash, Negar. Database alignment with gaussian features. *CoRR*.

[26] Dai, Osman Emre, Cullina, Daniel, Kiyavash, Negar, and Grossglauser, Matthias. On the performance of a canonical labeling for matching correlated erdős-rényi graphs. *CoRR abs/1804.09758* (2018).

[27] Dalipi, Fisnik, and Yayilgan, Sule Yildirim. Security and privacy considerations for IoT application on smart grids: Survey and research challenges. In *Future Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on* (2016), IEEE, pp. 63–68.

[28] Dewri, Rinku, and Thurimella, Ramakrisha. Exploiting service similarity for privacy in location-based search queries. *IEEE Transactions on Parallel and Distributed Systems 25*, 2 (2014), 374–383.

[29] Duckham, Matt, and Kulik, Lars. A formal model of obfuscation and negotiation for location privacy. In *International conference on pervasive computing* (2005), Springer, pp. 152–170.

[30] Dwork, Cynthia, Kenthapadi, Krishnaram, McSherry, Frank, Mironov, Ilya, and Naor, Moni. Our data, ourselves: Privacy via distributed noise generation. In *EUROCRYPT* (2006).

[31] Evans, Dave. The internet of things how the next evolution of the internet is changing everything. `https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf`, April,.

[32] Fortunato, Santo, and Hric, Darko. Community detection in networks: A user guide. *Physics Reports 656* (2016), 1–44.

[33] Freudiger, Julien, Raya, Maxim, Félegyházi, Márk, Papadimitratos, Panos, and Hubaux, Jean-Pierre. Mix-zones for location privacy in vehicular networks. In *CM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)* (2007).

[34] Freudiger, Julien, Shokri, Reza, and Hubaux, Jean-Pierre. On the optimal placement of mix zones. In *Privacy enhancing technologies* (2009), Springer, pp. 216–234.

[35] Fu, Xinzhe, Hu, Zhongzhao, Xu, Zhiying, Fu, Luoyi, and Wang, Xinbing. Deanonymization of social networks with communities: When quantifications meet algorithms. *CoRR abs/1703.09028* (2017).

[36] Gedik, Buğra, and Liu, Ling. Location privacy in mobile systems: A personalized anonymization model. In *Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on* (2005), IEEE, pp. 620–629.

[37] Geng, Junxian, Bhattacharya, Anirban, and Pati, Debdeep. Probabilistic community detection with unknown number of communities. *Journal of the American Statistical Association* (2018), 1–13.

[38] Girvan, Michelle, and Newman, Micaleah. Community structure in social and biological networks. *Proceedings of the National Academy of Sciences of the United States of America 99(12)* (2002), 7821–7826.

[39] Gruteser, Marco, and Grunwald, Dirk. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proceedings of the 1st international conference on Mobile systems, applications and services* (2003), ACM, pp. 31–42.

[40] Gruteser, Marco, and Grunwald, Dirk. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proceedings of the 1st international conference on Mobile systems, applications and services* (San Francisco, California, USA, 2003), ACM.

[41] Guo, Dongning, and Verdú, Sergio. Randomly spread cdma: Asymptotics via statistical physics. *arXiv preprint cs/0503063* (2005).

[42] Guo, Dongning, Zhu, Yan, and Honig, Michael L. Co-channel interference mitigation in multiuser systems with unknown channels. In *Proceedings of XXIXth URSI General Assembly* (2008).

[43] Gupta, Piyush, and Kumar, Panganmala R. The capacity of wireless networks. *IEEE Transactions on information theory 46*, 2 (2000), 388–404.

[44] Harris, Albert F, Sundaram, Hari, and Kravets, Robin. Security and privacy in public IoT spaces. In *Computer Communication and Networks (ICCCN), 2016 25th International Conference on* (2016), IEEE, pp. 1–8.

[45] Hoh, Baik, and Gruteser, Marco. Protecting location privacy through path confusion. In *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on* (2005), IEEE, pp. 194–205.

[46] Hoh, Baik, Gruteser, Marco, Xiong, Hui, and Alrabady, Ansaf. Preserving privacy in gps traces via uncertainty-aware path cloaking. In *Proceedings of the 14th ACM conference on Computer and communications security* (2007), ACM, pp. 161–171.

[47] Hosseinzadeh, Shohreh, Rauti, Sampsa, Hyrynsalmi, Sami, and Leppanen, Ville. Security in the internet of things through obfuscation and diversification. In *Computing, Communication and Security (ICCCS), IEEE Conference on* (2015), IEEE, pp. 123–124.

[48] Ji, Shouling, Li, Weiqing, Srivatsa, Mudhakar, and Beyah, Raheem A. Structural data de-anonymization: Quantification, practice, and implications. In *ACM Conference on Computer and Communications Security* (2014), pp. 1040–1053.

[49] Jog, Varun S., and Loh, Po-Ling. Recovering communities in weighted stochastic block models. pp. 1308–1315.

[50] Kalnis, Panos, Ghinita, Gabriel, Mouratidis, Kyriakos, and Papadias, Dimitris. Preventing location-based identity inference in anonymous spatial queries. *Knowledge and Data Engineering, IEEE Transactions on 19*, 12 (2007), 1719–1733.

[51] Kawamoto, Yusuke, and Murakami, Takao. Differentially private obfuscation mechanisms for hiding probability distributions. *CoRR abs/1812.00939* (2018).

[52] Kazemi, Ehsan. Network alignment: Theory, algorithms, and applications.

[53] Kazemi, Ehsan, Yartseva, Lyudmila, and Grossglauser, Matthias. When can two unlabeled networks be aligned under partial overlap? In *53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)* (Monticello, IL, USA, 2015).

[54] Kido, Hidetoshi, Yanagisawa, Yutaka, and Satoh, Tetsuji. An anonymous communication technique using dummies for location-based services. In *Pervasive Services, 2005. ICPS'05. Proceedings. International Conference on* (2005), IEEE, pp. 88–97.

[55] Kido, Hidetoshi, Yanagisawa, Yutaka, and Satoh, Tetsuji. Protection of location privacy using dummies for location-based services. In *Data Engineering Workshops, 2005. 21st International Conference on* (2005), IEEE, pp. 1248–1248.

[56] Kifer, Daniel, and Machanavajjhala, Ashwin. No free lunch in data privacy. In *Proceedings of the 2011 ACM SIGMOD International Conference on Management of data* (Athens, Greece, 2011), ACM, pp. 193–204.

[57] Kifer, Daniel, and Machanavajjhala, Ashwin. Pufferfish: A framework for mathematical privacy definitions.

[58] Lelarge, Marc, Massoulié, Laurent, and Xu, Jiaming. Reconstruction in the labelled stochastic block model. *IEEE Transactions on Network Science and Engineering 2*, 4 (2015), 152–163.

[59] Levy, Bernard C. *Principles of Signal Detection and Parameter Estimation*. 2008.

[60] Li, Huaxin, Zhu, Haojin, Du, Suguo, Liang, Xiaohui, and Shen, Xuemin. Privacy leakage of location sharing in mobile social networks: Attacks and defense. *IEEE Transactions on Dependable and Secure Computing PP*, 99 (2016).

[61] Li, K., Pishro-Nik, H., and Goeckel, D. L. Bayesian time series matching and privacy. In *51th Asilomar Conference on Signals, Systems and Computers* (Pacific Grove, CA, USA, 2017), IEEE.

[62] Li, K., Pishro-Nik, H., and Goeckel, D. L. Privacy under anonymization and obfuscation with gaussian series. In *Conference on Information Sciences and Systems (CISS)* (Princeton, NJ,USA, 2017), IEEE.

[63] Li, Ke, Pishro-Nik, Hossein, and Goeckel, Dennis L. Bayesian time series matching and privacy. In *2017 51st Asilomar Conference on Signals, Systems, and Computers* (2017), IEEE, pp. 1677–1681.

[64] Liao, Jiachun, Sankar, Lalitha, du Pin Calmon, Flávio, and Tan, Vincent Yan Fu. Hypothesis testing under maximal leakage privacy constraints. In *International Symposium on Information Theory (ISIT)* (Aachen, Germany, 2017), IEEE, pp. 779–783.

[65] Liao, Jiachun, Sankar, Lalitha, Tan, Vincent Y. F., and du Pin Calmon, Flávio. Hypothesis testing in the high privacy limit. *CoRR abs/1607.00533* (2016).

[66] Lin, Huichen, and Bergmann, Neil W. Iot privacy and security challenges for smart home environments. *Information 7*, 3 (2016), 44.

[67] Liu, Changchang, Mittal, Prateek, and Chakraborty, Supriyo. Dependence makes you vulnerable: Differential privacy under dependent tuples. In *23nd Annual Network and Distributed System Security Symposium* (San diego, CA, USA, 2016).

[68] Liu, Hai, Li, Xinghua, and Li, Hui. Spatiotemporal correlation-aware dummy-based privacy protection scheme for location-based services. In *IEEE Conference on Computer Communications (INFOCOM)* (2017), IEEE.

[69] Liu, Xinxin, Liu, Kaikai, Guo, Linke, Li, Xiaolin, and Fang, Yuguang. A game-theoretic approach for achieving k-anonymity in location based services. In *INFOCOM, 2013 Proceedings IEEE* (2013), IEEE, pp. 2985–2993.

[70] Lu, Hua, Jensen, Christian S, and Yiu, Man Lung. Pad: privacy-area aware, dummy-based location privacy in mobile services. In *Proceedings of the Seventh ACM International Workshop on Data Engineering for Wireless and Mobile Access* (2008), ACM, pp. 16–23.

[71] Ma, Zhendong, Kargl, Frank, and Weber, Michael. A location privacy metric for v2x communication systems. In *Sarnoff Symposium, 2009. SARNOFF'09. IEEE* (2009), IEEE, pp. 1–6.

[72] Mendes, Ricardo, and Vilela, João P. On the effect of update frequency on geo-indistinguishability of mobility traces. In *Proceedings of the 11th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (Stockholm, Sweden).

[73] Montazeri, Z., Houmansadr, A., and Pishro-Nik, H. Achieving Perfect Location Privacy in Wireless Devices Using Anonymization. *IEEE Transaction on Information Forensics and Security, to appear 12*, 11' (2017), 2683–2698.

[74] Naini, F., Unnikrishnan, J., Thiran, P., and Vetterli, M. Where you are is who you are: User identification by matching statistics. *IEEE Transactions on Information Forensics and Security 11*, 2 (2016), 358–372.

[75] Nilizadeh, Shirin, Kapadia, Apu, and Ahn, Yong-Yeol. Community-enhanced de-anonymization of online social networks. In *ACM Conference on Computer and Communications Security* (2014).

[76] Olteanu, Alexandra-Mihaela, Huguenin, Kévin, Shokri, Reza, Humbert, Mathias, and Hubaux, Jean-Pierre. Quantifying interdependent privacy risks with location data. *IEEE Transactions on Mobile Computing PP*, 99 (2016), 1–1.

[77] Onaran, Efe, Garg, Siddharth, and Erkip, Elza. Optimal de-anonymization in random graphs with community structure. In *2016 IEEE 37th Sarnoff Symposium* (Newark, NJ, USA, 2016), pp. 1–2.

[78] Ou, Lu, Qin, Zheng, Liu, Yonghe, Yin, Hui, Hu, Yupeng, and Chen, Hao. Multi-user location correlation protection with differential privacy. In *IEEE 22nd International Conference on Parallel and Distributed Systems (ICPADS)*, IEEE], year=2016, address= Wuhan, China.

[79] Oya, Simon, Troncoso, Carmela, and Pérez-González, Fernando. Is geo-indistinguishability what you are looking for? In *Proceedings of the 2017 on Workshop on Privacy in the Electronic Society* (Dallas, Texas, USA).

[80] Oya, Simon, Troncoso, Carmela, and Pérez-González, Fernando. A tabula rasa approach to sporadic location privacy. *CoRR abs/1809.04415* (2018).

[81] Palanisamy, Balaji, and Liu, Ling. Mobimix: Protecting location privacy with mix-zones over road networks. In *Data Engineering (ICDE), 2011 IEEE 27th International Conference on* (2011), IEEE, pp. 494–505.

[82] Palia, Abhinav, and Tandon, Rajat. Optimizing noise level for perturbing geo-location data. *Future of Information and Communication Conference* (2018), 63–73.

[83] Pedarsani, Pedram, Figueiredo, Daniel R., and Grossglauser, Matthias. A bayesian method for matching two similar graphs without seeds. In *51st Annual Allerton Conference on Communication, Control, and Computing (Allerton)* (Monticello, IL, USA, 2013), ACM.

[84] Porambag, Pawani, Ylianttila, Mika, Schmitt, Corinna, Kumar, Pardeep, Gurtov, Andrei, and Vasilakos, Athanasios V. The quest for privacy in the internet of things. *IEEE Cloud Computing*, 2 (2016).

[85] Report, FTC Staff. Internet of things: Privacy and security in a connected world.

[86] Saad, Hussein, and Nosratinia, Aria. Community detection with side information: Exact recovery under the stochastic block model. *IEEE Journal of Selected Topics in Signal Processing 12* (2018), 944–958.

[87] Sadeghi, Ahmad-Reza, Wachsmann, Christian, and Waidner, Michael. Security and privacy challenges in industrial internet of things. In *Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE* (2015), IEEE, pp. 1–6.

[88] Salamatian, Salman, Zhang, Amy, du Pin Calmon, Flavio, Bhamidipati, Sandilya, Fawaz, Nadia, Kveton, Branislav, Oliveira, Pedro, and Taft, Nina. How to hide the elephant-or the donkey-in the room: Practical privacy against statistical inference for large data. In *GlobalSIP* (2013), pp. 269–272.

[89] Sankar, Lalitha, Rajagopalan, S Raj, and Poor, H Vincent. Utility-privacy tradeoffs in databases: An information-theoretic approach. *Information Forensics and Security, IEEE Transactions on 8*, 6 (2013), 838–852.

[90] Scarlett, Jonathan, and Cevher, Volkan. Partial recovery bounds for the sparse stochastic block model. In *2016 IEEE International Symposium on Information Theory (ISIT)* (2016), IEEE, pp. 1904–1908.

[91] Shankar, Pravin, Ganapathy, Vinod, and Iftode, Liviu. Privately querying location-based services with sybilquery. In *Proceedings of the 11th international conference on Ubiquitous computing* (2009), ACM, pp. 31–40.

[92] Shirani, Farhad, Garg, Siddharth, and Erkip, Elza. Seeded graph matching: Efficient algorithms and theoretical guarantees. In *51st Asilomar Conference on Signals, Systems, and Computers* (Pacific Grove, CA, USA, 2017), pp. 253–257.

[93] Shirani, Farhad, Garg, Siddharth, and Erkip, Elza. Matching graphs with community structure: A concentration of measure approach. *2018 56th Annual Allerton Conference on Communication, Control, and Computing (Allerton)* (2018), 1028–1035.

[94] Shirani, Farhad, Garg, Siddharth, and Erkip, Elza. Typicality matching for pairs of correlated graphs. *2018 IEEE International Symposium on Information Theory (ISIT)* (2018), 221–225.

[95] Shirani, Farhad, Garg, Siddharth, and Erkip, Elza. A concentration of measure approach to database de-anonymization. *CoRR abs/1901.07655* (2019).

[96] Shokri, Reza, Theodorakopoulos, George, Danezis, George, Hubaux, Jean-Pierre, and Le Boudec, Jean-Yves. Quantifying location privacy: the case of sporadic location exposure. In *Privacy Enhancing Technologies* (2011), Springer, pp. 57–76.

[97] Shokri, Reza, Theodorakopoulos, George, Le Boudec, Jean-Yves, and Hubaux, Jean-Pierre. Quantifying location privacy. In *Security and Privacy (SP), 2011 IEEE Symposium on* (2011), IEEE, pp. 247–262.

[98] Shokri, Reza, Theodorakopoulos, George, Papadimitratos, Panos, Kazemi, Ehsan, and Hubaux, Jean-Pierre. Hiding in the mobile crowd: Locationprivacy through collaboration. *IEEE transactions on dependable and secure computing 11*, 3 (2014), 266–279.

[99] Shokri, Reza, Theodorakopoulos, George, Troncoso, Carmela, Hubaux, Jean-Pierre, and Le Boudec, Jean-Yves. Protecting location privacy: optimal strategy against localization attacks. In *Proceedings of the 2012 ACM conference on Computer and communications security* (2012), ACM, pp. 617–627.

[100] Singhal, Kushagra, Cullina, Daniel, and Kiyavash, Negar. Significance of side information in the graph matching problem. *CoRR abs/1706.06936* (2017).

[101] Sivaraman, Vijay, Gharakheili, Hassan Habibi, Vishwanath, Arun, Boreli, Roksana, and Mehani, Olivier. Network-level security and privacy control for smart-home IoT devices. In *Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on* (2015), IEEE, pp. 163–167.

[102] Soltani, R., Goeckel, D., Towsley, D., and Houmansadr, A. Towards provably invisible network flow fingerprints. In *2017 51st Asilomar Conference on Signals, Systems, and Computers* (Oct 2017), pp. 258–262.

[103] Soltani, R., Goeckel, D., Towsley, D., and Houmansadr, A. Fundamental limits of invisible flow fingerprinting. *arXiv preprint arXiv* (2018).

[104] Song, Shuang, Wang, Yizhen, and Chaudhuri, Kamalika. Pufferfish privacy mechanisms for correlated data. In *Proceedings of the 2017 ACM International Conference on Management of Data* (Chicago, Illinois, USA, 2017), ACM, pp. 1291–1306.

[105] Sweeney, Latanya. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10*, 05 (2002), 557–570.

[106] Takbiri, N., Houmansadr, A., Goeckel, D.L., and Pishro-Nik, H. Fundamental limits of location privacy using anonymization. In *Annual Conference on Information Science and Systems (CISS)* (2017), IEEE.

[107] Takbiri, N., Houmansadr, A., Goeckel, D.L., and Pishro-Nik, H. Asymptotic limits of privacy in bayesian time series matching. In *53rd Annual Conference on Information Science and Systems (CISS)* (Baltimore, MD, USA, 2019), IEEE.

[108] Takbiri, Nazanin, Houmansadr, Amir, Goeckel, Dennis L., and Pishro-Nik, Hossein. Privacy of dependent users against statistical matching. *submitted to IEEE Transactions on Information Theory, Available at https://arxiv.org/abs/1710.00197*.

[109] Takbiri, Nazanin, Houmansadr, Amir, Goeckel, Dennis L., and Pishro-Nik, Hossein. Limits of location privacy under anonymization and obfuscation. In *International Symposium on Information Theory (ISIT)* (Aachen, Germany, 2017), IEEE, pp. 764–768.

[110] Takbiri, Nazanin, Houmansadr, Amir, Goeckel, Dennis L., and Pishro-Nik, Hossein. Privacy against statistical matching: Inter- user correlation. In *International Symposium on Information Theory (ISIT)* (Vail, Colorado, USA, 2018).

[111] Takbiri, Nazanin, Houmansadr, Amir, Goeckel, Dennis L., and Pishro-Nik, Hossein. Matching anonymized and obfuscated time series to users' profiles. *IEEE Transactions on Information Theory 65*, 2 (2019), 724–741.

[112] Takbiri, Nazanin, Li, Ke, Goeckel, Dennis L., and Pishro-Nik, Hossein. Statistical matching in the presence of anonymization and obfuscation: Non-asymptotic results in the discrete case. In *52nd Annual Conference on Information Science and Systems (CISS)* (Princeton,NJ, USA, 2018), IEEE.

[113] Takbiri, Nazanin, Shejwalker, Virat, Houmansadr, Amir, Goeckel, Dennis L., and Pishro-Nik, Hossein. Leveraging prior knowledge asymmetries in the design of location privacy-preserving mechanisms. *Submitted to IEEE Wireless Communications Letter* (2020).

[114] Takbiri, Nazanin, Soltani, Ramin, Goeckel, Dennis, Houmansadr, Amir, and Pishro-Nik, Hossein. Asymptotic loss in privacy due to dependency in gaussian traces. In *IEEE Wireless Communications and Networking Conference (WCNC)* (Marrakech, Morocco, 2019), IEEE.

[115] Ukil, Arijit, Bandyopadhyay, Soma, and Pal, Arpan. IoT-privacy: To be private or not to be private. In *Computer Communications Workshops (INFOCOM WKSHPS), IEEE Conference on* (2014), IEEE, pp. 123–124.

[116] Ukil, Arijit, Bandyopadhyay, Soma, and Pal, Arpan. Privacy for IoT: Involuntary privacy enablement for smart energy systems. In *Communications (ICC), 2015 IEEE International Conference on* (2015), IEEE, pp. 536–541.

[117] Um, Jung-Ho, Kim, Hee-Dae, and Chang, Jae-Woo. An advanced cloaking algorithm using hilbert curves for anonymous location based service. In *Social Computing (SocialCom), 2010 IEEE Second International Conference on* (2010), IEEE, pp. 1093–1098.

[118] Unnikrishnan, Jayakrishnan. Asymptotically optimal matching of multiple sequences to source distributions and training sequences. *IEEE Transactions on Information Theory 61*, 1 (2015), 452–468.

[119] Verdú, Sergio, and Shamai, Shlomo. Spectral efficiency of cdma with random spreading. *IEEE Transactions on Information theory 45*, 2 (1999), 622–640.

[120] Vosoughi, M.A., and Köse, S. Combined distinguishers to enhance the accuracy and success of side channel analysis. In *IEEE International Symposium on Circuits and Systems* (May 2019), pp. 1–5.

[121] Wan, Cong, Peng, Sancheng, Wang, Cong, and Yuan, Ying. Communities detection algorithm based on general stochastic block model in mobile social networks. pp. 178–185.

[122] Wang, Hao, and du Pin Calmon, Flávio. An estimation-theoretic view of privacy. *CoRR abs/1710.00447* (2017).

[123] Warner, Stanley L. Randomized response: A survey technique for eliminating evasive answer bias. *Journal of the American Statistical Association 60*, 309 (1965), 63–69.

[124] Wernke, Marius, Skvortsov, Pavel, Dürr, Frank, and Rothermel, Kurt. A classification of location privacy attacks and approaches. *Personal and Ubiquitous Computing 18*, 1 (2014), 163–175.

[125] Wu, Xinyu, Hu, Zhongzhao, Fu, Xinzhe, Fu, Luoyi, Wang, Xinbing, and Lu, Songwu. Social network de-anonymization with overlapping communities: Analysis, algorithm and experiments. *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications* (2018), 1151–1159.

[126] Xiao, Yonghui, and Xiong, Li. Protecting locations with differential privacy under temporal correlations. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 1298–1309.

[127] Yamamoto, Hirosuke. A source coding problem for sources with additional outputs to keep secret from the receiver or wiretappers (corresp.). *IEEE Transactions on Information Theory 29*, 6 (1983), 918–923.

[128] Yang, Bin, Sato, Issei, and Nakagawa, Hiroshi. Bayesian differential privacy on correlated data. In *Proceedings of the 2015 ACM SIGMOD International Conference on Management of Data* (Melbourne, Victoria, Australia, 2015), ACM, pp. 747–762.

[129] Yartseva, Lyudmila, and Grossglauser, Matthias. On the performance of percolation graph matching. In *Proceedings of the first ACM conference on Online social networks* (Boston, Massachusetts, USA, 2013), ACM, pp. 119–130.

[130] Zhang, Jun, Cormode, Graham, Procopiuc, Cecilia M., Srivastava, Divesh, and Xiao, Xiaokui. Privbayes: Private data release via bayesian networks. In *Proceedings of the 2014 ACM SIGMOD International Conference on Management of Data*, pp. 1423–1434.

[131] Zhang, Shanfeng, Ma, Qiang, Zhu, Tong, Liu, Kebin, Zhang, Lan, He, Wenbo, and Liu, Yunhao. Plp: Protecting location privacy against correlation-analysis attack in crowdsensing. In *44th International Conference on Parallel Processing (ICPP)* (Beijing, China, 2015), IEEE.

[132] Zhang, Xuejun, Gui, Xiaolin, Tian, Feng, Yu, Si, and An, Jian. Privacy quantification model based on the bayes conditional risk in location-based services. *Tsinghua Science and Technology 19*, 5 (2014), 452–462.

[133] Zhang, Yuan, Tong, Wei, and Zhong, Sheng. On designing satisfaction-ratio-aware truthful incentive mechanisms for k-anonymity location privacy. *IEEE Transactions on Information Forensics and Security 11*, 11 (2016), 2528–2541.

[134] Zhong, Ge, and Hengartner, Urs. A distributed k-anonymity protocol for location privacy. In *Pervasive Computing and Communications, 2009. PerCom 2009. IEEE International Conference on* (2009), IEEE, pp. 1–10.

[135] Zhu, Tianqing, Xiong, Ping, Li, Gang, and Zhou, Wanlei. Correlated differential privacy: Hiding information in non-iid data set. *IEEE Transactions on Information Forensics and Security 10*, 2 (2015), 229–242.

[136] Zurbaran, Mayra Alejandra, Avila, Karen, Wightman, Pedro, and Fernandez, Michael. Near-rand: Noise-based location obfuscation based on random neighboring points. *IEEE Latin America Transactions 13*, 11 (2015), 3661–3667.