

Received November 16, 2020, accepted November 26, 2020, date of publication December 2, 2020,  
date of current version December 14, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3041854

# A Privacy-Preserving Game Model for Local Differential Privacy by Using Information-Theoretic Approach

NINGBO WU<sup>1</sup>, CHANGGEN PENG<sup>1,2</sup>, AND KUN NIU<sup>1</sup>

<sup>1</sup>College of Computer Science and Technology, Guizhou Big Data Academy, Guizhou University, Guiyang 550025, China

<sup>2</sup>State Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025, China

Corresponding author: Changgen Peng (cgpeng@gzu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant U1836205 and Grant 61662009, in part by the 13th Five-Year National Cryptography Development Foundation under Grant MMJJ20170129, in part by the Science and Technology Program of Guizhou Province (Guizhou Science Contract Major Program) under Grant [2018]3001, in part by the Guizhou Science Contract Platform Talent under Grant [2020]5017, in part by the Project of Innovative Group in Guizhou Education Department under Grant [2013]09, and in part by the Research Fund Project for Graduate Students of Guizhou Province under Grant KYJJ2017005.

**ABSTRACT** Local differential privacy (LDP) is an effective privacy-preserving model to address the problems which do not have a trusted entity. The main idea of the LDP is to add randomness in real data to guarantee individual's private sensitive information. Here, the technology of randomized response is an effective method to realize the LDP mechanism. In fact, the randomized response is a probabilistic mapping from the real data to perturbed data, which can be modeled as an information-theoretic lossy compression mechanism. What's more, the privacy budget  $\epsilon$  has become a *de facto* standard to quantify the worst-case privacy leakage. However, such a metrics can not capture the question that which one is the optimal privacy mechanism in a set of equivalent  $\epsilon$ -privacy mechanisms. Besides, the privacy and utility are closely correlated with the privacy mechanism, and existing methods do not consider the strategic adversary's behavior. In this paper, we tackle the problem of tradeoffs privacy and utility under the rational framework within an information-theoretic approach as the metrics. To address the problem, we first formulate this trade-off as a minimax information leakage problem. Then, we propose a privacy preserving attack and defense (PPAD) game framework, that is, a two-person zero-sum (TPZS) game. Further, we develop an alternating optimization algorithm to compute the saddle point of the proposed PPAD game. As a case study, we apply our method to compare several alternative  $\ln 2$ -privacy mechanisms, the experimental result demonstrates that can provide an effective method to compare equivalent  $\epsilon$ -privacy mechanisms. Furthermore, the numeric simulation result confirms that the proposed method also be useful for the protector to assess privacy disclosure risks.

**INDEX TERMS** Privacy-preserving, information-theoretic utility, mutual information privacy leakage, minimax game, local differential privacy.

## I. INTRODUCTION

The problem of leaking private sensitive information is widely concerned with society and academia, and is becoming one of the main challenges in today's big data era. The privacy issues bring the demands of privacy protection for data collection, data release as well as data analysis, which urgently need the effective privacy protection models and

algorithms. Specifically, the differential privacy (DP) [1], [2] is a privacy protocol, which provides rigorous data privacy guarantees. In fact, the DP has become a *de facto* standard for privacy-preserving community because it has a rigorous mathematical proof of privacy guarantees. In general, DP is classified as two working settings, i.e., centralized setting and local setting. In the centralized setting [2], a trusted data curator performs the privacy protocol to protect sensitive data records. The basic idea is to add randomness to the accurate results. However, there is not always having the

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Asif<sup>1</sup>.

trustable data curator who processes the data. To this end, local differential privacy [3] (LDP) is proposed to address the problem of untrustworthy data curator. In the LDP, each user perturbs her real data locally before sending reported data to the data aggregator. The original motivation of the LDP is achieved by randomized response, which was first discussed in [4]. In recent years, many state-of-the-art LDP mechanisms have been developed (e.g., randomized aggregatable privacy-preserving ordinal response, RAPPOR [5], [6],  $k$ -ary randomized response,  $k$ -RR [7]) to provide privacy preserving. Currently, the LDP is widely investigated in the privacy protection area, and has been applied into privacy-preserving data collecting and analyzing, such as Google Chrome browser [5], Apple's OS [8] etc.

Specifically, each user independently sends her own reported data to the aggregator in the data collection scenario. Afterwards, the aggregator collects, stores these reported data, and then prefers to infer the individual's information from the collected data since he may be an *honest-but-curious* adversary. In such case, each user performs LDP locally to protect her privacy. In practice, the randomized response (RR) technique is an effective method to achieve LDP [7], [9]–[11]. Essentially the RR mechanism is a probabilistic mapping from real data to disguised data. Thus the randomness of privacy-preserving mechanism corresponds to the problem of trade-off between privacy protection and data accuracy, which is the well-known problem of privacy-utility trade-off. At present, this problem is still the concern of academic research.

Indeed, the LDP mechanism can be modeled as a noisy channel from the perspective of private information flow [12], [13]. Meanwhile, privacy and utility metrics are the fundamental work to investigate the privacy-utility trade-off. Currently, the privacy budget  $\epsilon$  is a de facto standard to quantify the indistinguishability level. However, it still has its drawbacks. As mentioned in [14], a deterministic privacy protocol  $Q(x) = x \bmod 2$  which provides privacy guarantee with  $\epsilon$  is infinity, but it still prevents some privacy disclosure. In addition, such a metrics can not evaluate equivalent  $\epsilon$ -indistinguishability mechanisms. To solve these drawbacks, information-theoretic approach is used to measure privacy leakage, and has been widely studied in recent years [7], [15]–[18]. The mutual information (MI) measures how much information about real data is contained in disguised data. It captures the aggregators' knowledge, and assumes aggregator does not know the true distribution exactly, but only knows it lies in a probability distribution set [7], [13]. The MI has its advantage to solve this problem. In fact, the users aim to reduce privacy leakage, they are analogous to privacy defender. However, the goal of an aggregator is to obtain the privacy statistics information and attempts to infer personal information, who is similar to privacy attacker. Thus, the concerned problem evolves into a privacy attack-defense game between attacker and defender.

Based on those analyses mentioned above, the objective of this paper is to seek an optimal privacy mechanism by

analyzing the actions of privacy attacker and defender. Intuitively, the more randomness of the privacy mechanism will be obtained the better privacy performance. The works [16], [18], [19] utilize MI measuring the privacy leakage about privacy-preserving mechanisms because the notion of MI has a clear meaning, that is, measuring the amount of uncertainty reduction about original information. However, the works [7], [20] adopt MI as utility metrics, and further preserve the useful information as much as possible. Inspired by these works, the problem mentioned above would become a minimax problem, and naturally evolved into a two-person zero-sum game. In this paper, we consider formalizing the concerned problem as an attack and defense game about privacy since the game theory has its advantages to deal with such a problem. Then, we provide the analytic results, which confirm that our method can be used for privacy defender to take optimal privacy strategy.

#### A. OUR CONTRIBUTION

The major contributions of our work can be summarized as follows:

- 1) To analyze the rational actions between users and aggregator, we propose a general game-theoretic framework of privacy attack and defense, PPAD, and quantify the private information gain of aggregator based on the information-theoretic approach.
- 2) We formalize the objectives of privacy defender and attacker as a minimax MI privacy problem, and then construct a two-person zero-sum game to solve the formalized minimax problem.
- 3) We propose an effective method to evaluate equivalent  $\epsilon$ -privacy mechanisms. Further, we demonstrate the MI privacy leakage can reach the upper bound under the worst-case, and that can be used to assess privacy disclosure risks.

#### B. PAPER OUTLINE

The remainder of this paper is organized as follows. Section II reviews the related work about our research topic, and Section III introduces the preliminaries to the paper. Section IV presents the system model and problem formalization. Section V describes the details of privacy attack and defense game model, and presents its theoretic analysis. A case study and numerical simulation results are given in Section VI, followed by the conclusion and future work in Section VII.

#### II. RELATED WORK

Differential privacy (DP), has been widely studied in a series of state-of-the-art literatures (e.g., [1], [2], [21], [22]). In recent years, many researchers began to measure privacy leakage and usability with information-theoretic approach (e.g., [13], [17], [23]), which is used to investigate the optimal DP mechanism. What's more, utility-privacy tradeoffs has been became an important problem in the privacy-preserving

community. In addressing this problem, the game theoretic idea is used to study it under the DP becoming a fascinating research topic. In the following, we survey the important works in each aspect.

Firstly, the privacy-preserving mechanism can be modeled as a noisy channel model [13], [17], [23], [24], including the radio channel model [25] connected with IoT devices. Then, the privacy leakage can be measured by entropy [19], [26], [27]. In particular, Alvim *et al.* proposed measure information uncertainty based on the idea of quantitative information flow (QIF). Moreover, the notion of *mutual information* has also been considered in [15], [18], [28], and given a formal definition of MI-privacy. Wang *et al.* [18] formulated a MI-privacy optimization program, and proved that the MI optimal mechanism guarantees a certain level of differential privacy. In addition, Cuff *et al.* [28] adopted MI given an equivalent definition of differential privacy. The works of [15] and [29] given a fundamental relation between MI and differential privacy.

Secondly, the information-theoretic approach has also been used in the LDP setting. It is indeed true that the LDP can be represented by a probabilistic mapping from original data domain  $\mathcal{X}$  to a regenerated space  $\mathcal{Y}$ . Let  $Q(y|x)$  be the conditional probability of input  $x \in \mathcal{X}$  and output  $y \in \mathcal{Y}$ . As such, the LDP mechanism is captured by a conditional probability  $Q$  (s.t.  $\sum_y Q(\cdot|x) = 1$  and  $Q(\cdot|x) \geq 0$ ). In this line of research, [7] proposed  $k$ -RR mechanism by using MI as utility metrics. Also, [7], [30] proposed  $k$ -RR mechanism is optimal with the probability  $Q(y|x) = \frac{\epsilon^e}{|\mathcal{X}| + \epsilon^e - 1}$  for all  $x = y$ , and  $Q(y|x) = \frac{1}{|\mathcal{X}| + \epsilon^e - 1}$  for  $x \neq y$ . As such, the LDP established a fundamental relation with information-theoretic noisy channel model, and also represented by a probability transfer matrix. Based on this fundamental relation, [14] presented a new metrics approach for LDP from information-theoretic perspective. Besides, [13], [17] investigated the optimal LDP mechanism using information-theoretic approach. In summary, the information-theoretic approach which applied into the LDP has attracted lots of attentions.

Finally, game theory as an effective analysis tool for the issue that existing conflict and competition, has been widely studied in data security recent years (e.g., [31]–[33]). In the application of differential privacy, Xiao *et al.* [34] formulated a privacy aware recommendation game to evaluate the performance of the proposed deep reinforcement learning based user profile perturbation scheme, which applies differential privacy to protect user privacy within recommendation services. Besides, the well known two-player zero-sum game model has been considered by [35]–[37]. What's more, [36]–[38] considered information leakage game model, which are constructed from the perspective of QIF. Additionally, the non-cooperative differential game [39] and the Stackelberg game [40] have been studied in privacy-preserving under differential privacy. From these related work about the game and privacy preserving, we can conclude that the problem of utility-privacy trade-off solved by game-theoretic approach is becoming an effective method.

### III. PRELIMINARIES

In this section, some basics will be summarized for our usage in this paper for readers' convenience. Here, we only give a brief introduction because of space limitation, if readers need, refer to the relevant materials for more details.

#### A. LOCAL DIFFERENTIAL PRIVACY SETTING

Let  $X$  be a discrete random variable, which takes its value from a candidate set  $\mathcal{X}$ , and  $x \in \mathcal{X}$  represents user's private data. In order to protect the secret data, a randomized privacy-preserving mechanism will be used to produce a disguised data. We assume the disguised data is a discrete random variable  $Y$ , and its value  $y$  comes from a candidate set  $\mathcal{Y}$ . Thus the privacy-preserving mechanism forms a probabilistic mapping from  $\mathcal{X}$  to  $\mathcal{Y}$ . In fact, DP has an underlying assumption, i.e., there is a trusted data curator who has the real data. However, it is generally a semi-honest participant who follows the privacy protocol, but attempts to obtain private information. In such case, each user locally perturbs her original data to obtain disguised data, and then sends it to the aggregator. As such, the randomized mechanism is an uncertain function mapping  $Q(y|x)$ . Thus, we give the following equivalent definition.

*Definition 1 (Local differential privacy, LDP):* Let  $\mathcal{X}$  and  $\mathcal{Y}$  are finite discrete sets, a probabilistic function  $Q$  mapping  $\mathcal{X}$  to  $\mathcal{Y}$ , denoted as  $Q(y|x)_{y \in \mathcal{Y}, x \in \mathcal{X}} : \mathcal{X} \rightarrow \mathcal{Y}$ . It is a  $\epsilon$ -LDP mechanism, if and only if it satisfies

$$Q(y|x) \leq e^\epsilon Q(y|x'), \quad (1)$$

for all  $x, x' \in \mathcal{X}$  and  $y \in \mathcal{Y}$ . Further, the privacy budget  $\epsilon$  is a positive real number, which is defined as

$$\epsilon = \max_{x, x' \in \mathcal{X}, y \in \mathcal{Y}} \left\{ \ln \frac{Q(y|x)}{Q(y|x')} \right\}. \quad (2)$$

In particular, the privacy budget  $\epsilon$  describes the strength of privacy preserving as well as provides a quantitative method to measure privacy leakage. A natural question is: how does the privacy budget affect the privacy leakage? Intuitively, the  $\epsilon$  is a metrics, which measure the probabilistic distinguishability level of obtaining same output for any two distinct inputs. Further, a smaller  $\epsilon$  demonstrates a greater indistinguishability, that is, the attacker can hardly completely identify  $x$ . Thus leading to less privacy leakage.

*Remark 1:* The definition 1 shows that LDP provides the worst-case privacy guarantee, and the privacy budget  $\epsilon$  is independent with source probability distribution  $P(x)$  but only depends on the conditional probability  $Q(y|x)$ .

#### B. INFORMATION-THEORETIC METRICS

Let  $X$  and  $Y$  are discrete random variables, and  $X \in \mathcal{X}$ ,  $Y \in \mathcal{Y}$ . Therefore, a probabilistic function  $Q$  maps  $\mathcal{X}$  to  $\mathcal{Y}$  forming a typical *Shannon* [41] discrete noise channel  $Q : \mathcal{X} \times \mathcal{Y} \rightarrow \mathbb{R}$ , which is represented by a probability matrix  $Q(y|x)$  (s.t.  $0 \leq Q(y|x) \leq 1$  and  $\sum_{y \in \mathcal{Y}} Q(y|x) = 1$  for all  $y \in \mathcal{Y}$  and  $x \in \mathcal{X}$ ).

The notion of *entropy* is proposed to measure the uncertainty about random variable  $X$ . In particular, *Shannon entropy* [41], [42] is a popular metrics method, and which is defined as  $H(X) = -\sum_{x \in \mathcal{X}} P(x) \log P(x)$ . Then, the notion of *conditional entropy* defines the remaining uncertainty about  $X$  after observing  $Y$ , denoted as  $H(X|Y) = \mathbb{E}_{y \in \mathcal{Y}}[H(X|Y=y)]$ . Further, the mutual information  $I(X; Y)$  measures the amount of uncertainty reduction about  $X$ , i.e., the amount of information has learned from  $X$  by knowing  $Y$ , denoted as  $I(X; Y) = H(X) - H(X|Y)$ . More specifically,  $I(X; Y)$  quantifies how much information flow from  $X$  to  $Y$ , that is the basic idea of QIF [24]. Therefore, MI has an important property, that is, it will always be nonnegative. Furthermore, the relation between entropy and MI indicates that it can be calculated by

$$I(X; Y) = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} P(x)Q(y|x) \log \left( \frac{Q(y|x)}{P(y)} \right), \quad (3)$$

where  $P(y) = \sum_x P(x)Q(y|x)$ .

In addition, MI as an information measure method, it considers the influences of  $Q(y|x)$  as well as the *prior* distribution  $P(x)$ . That is to say, it reflects the statistical characteristics of the specific noisy channel.

### C. TWO-PERSON ZERO-SUM GAME AND MINIMAX THEOREM

Next, we consider a two-person attack and defense game, that is, a game between attacker and defender. Formally, such a game is defined as  $(\mathcal{D}, \mathcal{A}, u_{\mathcal{D}}, u_{\mathcal{A}})$ , of which  $\mathcal{D}$ ,  $\mathcal{A}$  be nonempty finite sets, and represent *defender's* and *attacker's* available actions, respectively. Furthermore, the measure functions  $u_{\mathcal{D}} : \mathcal{D} \times \mathcal{A} \rightarrow \mathbb{R}$  and  $u_{\mathcal{A}} : \mathcal{D} \times \mathcal{A} \rightarrow \mathbb{R}$  map the Cartesian product of  $\mathcal{D}$  and  $\mathcal{A}$  to a real number. More specifically, they are *payoff functions* of *defender* and *attacker*, respectively.

In addition, the players of a game always be assumed as rational decision makers, and they pursue to maximize their payoff functions. In particular, for any  $s_d \in \mathcal{D}$  and  $s_a \in \mathcal{A}$ , the sum of payoff function  $u_d(s_d, s_a)$  and  $u_a(s_d, s_a)$  equals to zero, i.e., the *defender's* loss is equivalent to the *attacker's* gain. Thus, the goal of attacker is to maximize the payoff function, while the defender is to minimize it. Usually, the two-person zero-sum game always corresponds to the minimax problem. As for this situation, the well-known *von Neumann's minimax theorem* [43] provides an effective analysis method. In the following, we give a brief introduction.

**Theorem 1 (von Neumann's minimax theorem):** Let  $\mathcal{P}$  and  $\mathcal{Q}$  be nonempty compact, convex subsets of Euclidean space, and  $U : \mathcal{P} \times \mathcal{Q} \rightarrow \mathbb{R}$  be a continuous function. If  $U(P, Q)$  is quasiconcave for all  $P \in \mathcal{P}$  and quasiconvex for all  $Q \in \mathcal{Q}$ . Then it has

$$\max_{P \in \mathcal{P}} \min_{Q \in \mathcal{Q}} U(P, Q) = \min_{Q \in \mathcal{Q}} \max_{P \in \mathcal{P}} U(P, Q) \quad (4)$$

The notion of *saddle point* is related to minimax Theorem 1, that is to say, if  $P^* \in \mathcal{P}$ ,  $Q^* \in \mathcal{Q}$  be the *saddle*

point of  $U(P, Q)$ , when they satisfy

$$U(P, Q^*) \leq U(P^*, Q^*) \leq U(P^*, Q) \quad (5)$$

for all  $P \in \mathcal{P}$  and  $Q \in \mathcal{Q}$ . This is equivalent to say,

$$\begin{cases} U(P^*, Q^*) = \sup_{P \in \mathcal{P}} U(P, Q^*) \\ U(P^*, Q^*) = \inf_{Q \in \mathcal{Q}} U(P^*, Q). \end{cases} \quad (6)$$

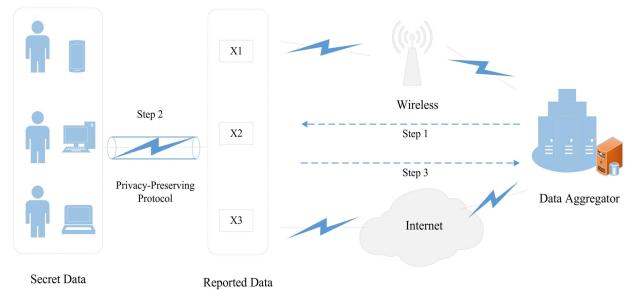
Then,  $(P^*, Q^*)$  is called as the *saddle point* of function  $U(P, Q)$  in  $\mathcal{P} \times \mathcal{Q}$ .

## IV. PROBLEM STATEMENT

In this section, we introduce the data collection architecture of this paper, and then establish its system model. Further, we formally define our research problem.

### A. APPLICATION ARCHITECTURE

Our application architecture is depicted in Figure 1, where a number of users and an aggregator participate in the data process procedures. To protect personal privacy, each user performs the privacy-preserving protocol to perturb her own secret data. In fact, an informed aggregator may know something a priori about the data distribution. To capture this priori, we assume he only knows the distribution lies in a set but does not know it exactly. In this situation, users and aggregator are considered as rational players, and they decide the privacy mechanism together. When the protocol has to be agreed, the process of the privacy-preserving data collection follows three steps.



**FIGURE 1.** The application architecture of privacy-preserving data collection.

**Step 1:** The aggregator releases a signal of data collection task, and determines the details of data to be collected. The data to be collected might include individual data such as home address, marital status. Then, the aggregator recruits users to report their own data.

**Step 2:** We consider the rational decision makers that they can decide whether or not they will report their data to the aggregator. If a user agrees to participate the current collection task, she performs the privacy protocol to derive reported data, and then sends it to the aggregator.

**Step 3:** Based on steps 1 and 2, the data aggregator collects, stores users' reported data, and then analyzes these collected data.

**Problem:** We consider an honest-but-curious aggregator who follows the privacy-preserving protocol but desires to infer personal information from the reported data. Thus our objective is to seek an optimal privacy mechanism to trade-off privacy and usability, that is, an optimization mechanism both for user and aggregator.

## B. SYSTEM MODEL

We consider there are  $n$  users in the privacy-preserving data collection system,  $[n] = \{1, 2, \dots, n\}$ ,  $\mathcal{X}$  (resp.  $\mathcal{Y}$ ) be a finite set that represents all possible values of personal data (resp. disguised data). Let  $X$  (resp.  $Y$ ) be a discrete random variable representing an individual's data (resp. disguised data). Furthermore, let  $|\mathcal{X}|$  be the number of distinct atoms in  $\mathcal{X}$ , and use a set of integers increase from 1 to  $|\mathcal{X}|$  to represent the real ordinal number in  $\mathcal{X}$ . The LDP forms a probabilistic function which maps  $x \in \mathcal{X}$  to  $y \in \mathcal{Y}$  with probability  $Q(y|x)$ , denoted as  $Q : \mathcal{X} \rightarrow \mathcal{Y}$ . In addition, we use the subscript  $x_i$  (resp.  $y_i$ ) to represent the personal data (resp. disguised data) of  $i$ th user in some cases.

To protect personal privacy, each user perturbs her own data independently, and then sends the disguised data to an aggregator. Generally, the obfuscation mechanism corresponds to a noisy channel because  $\epsilon$ -LDP is defined by a probabilistic function. In this way, a fundamental correlation has been established between LDP and information theory. To better illustrate this correlation, we first give the following example.

**Example 1:** For the problem with “yes” or “no” opinions, it captured by a binary candidate set with  $\{0, 1\}$ . In this case, the obfuscation mechanism can be considered as a binary crossover channel. For instance,  $Q_{(0|0)} = Q_{(1|1)} = 0.7$  and  $Q_{(1|0)} = Q_{(0|1)} = 0.3$ , then it satisfies  $\epsilon = \ln(7/3)$  local differential privacy.

Let  $P$  be an arbitrary probability distribution on discrete set  $\mathcal{X}$ , and  $\mathcal{P}$  be a finite set representing all possible probability distributions, denoted as  $P \in \mathcal{P}$ . We assume that each personal data to be drawn independently from a potential distribution  $P \in \mathcal{P}$  that it is not known by the aggregator but only knows the true distribution lies in  $\mathcal{P}$ . Further, we consider strategic users and aggregator that know the strategic space of each other. In this case, an honest-but-curious aggregator aims to maximize the success probability of privacy inference. For convenience, some notations used in this paper are listed in Table 1.

## C. MINIMAX PRIVACY PROBLEM

The privacy budget  $\epsilon$  of LDP is a *de facto* standard for measuring privacy level. However, we noticed that the notion of  $\epsilon$ -LDP provides the worst-case privacy guarantee, that is, it has the strongest hypothesis of background knowledge for privacy attacker. Thus, this metrics has its drawbacks [14] in some cases, since  $\epsilon$  is only determined by the probabilistic function mapping (defined by definition 1). If a set of privacy mechanisms all provide  $\epsilon$ -privacy guarantee, then the  $\epsilon$ -metrics can not distinguish which mechanism is better

**TABLE 1. Summary of Symbols and Notations.**

$n$	The total number of users
$\mathcal{X}, \mathcal{Y}$	Set of personal data, disguised data
$X, Y$	Discrete random variables representing personal data, disguised data
$ \mathcal{X} ,  \mathcal{Y} $	Number of distinct atoms in $\mathcal{X}, \mathcal{Y}$
$P, Q$	Probability distribution, probabilistic function of privacy mechanism
$\mathcal{D}, \mathcal{A}$	Strategic set of the defender $D$ and attacker $A$
$s_d, s_a$	Possible values of $\mathcal{D}, \mathcal{A}$
$U(\cdot, \cdot)$	Utility function of the game
$\mathcal{P}, \mathcal{Q}$	Set of probability distributions, available privacy mechanisms
$P^i, Q^i$	The $i$ th probability distribution of $\mathcal{P}$ , and the $i$ th privacy mechanism of $\mathcal{Q}$
$Q_{y x}^i$	Conditional probability distribution of $i$ th privacy mechanism in $\mathcal{Q}$
$P(\cdot)$	Priori probability distribution
$P^*, Q^*$	Optimal strategy of $D, A$
$P(\cdot  \cdot), Q(\cdot  \cdot)$	Conditional probability distribution

than others. In many applications, the qualities of privacy protection for these mechanisms need to be evaluated. The information-theoretic approach is an effective way to solve this problem. We present the method in details, which begins with a definition.

**Definition 2 (Equivalent  $\epsilon$ -privacy mechanisms):** Let  $\mathcal{Q}$  be a finite set representing a set of privacy-preserving mechanisms where contains  $k$  mechanisms. If each mechanism  $Q^i : \mathcal{X} \rightarrow \mathcal{Y}$  (s.t.  $1 \leq i \leq k$ ) of  $\mathcal{Q}$  is a  $\epsilon$ -privacy mechanism, then these mechanisms are called equivalent  $\epsilon$ -privacy mechanisms.

**Remark 2:** The condition of definition 2 can be relaxed to obtain a relaxing LDP mechanism set, that is, an arbitrary privacy mechanism  $Q^i \in \mathcal{Q}$  is  $\epsilon_i$ -LDP mechanism.

In fact, the privacy mechanism  $Q^i : \mathcal{X} \rightarrow \mathcal{Y}$  is a lossy compression mechanism, which controls how many bits of private information flowing from real data to disguised data. To quantify the amount of information, we borrow an information-theoretic method, and define the aggregator's information gain as

**Definition 3:** For a given private information  $x_i$ , the probability distribution  $P(X = x_i)$  and  $P(X = x_i | Y = y_i)$  represent the prior and posterior distribution after observing  $y_i$ , respectively. The ratio  $\log\left(\frac{P(X=x_i|Y=y_i)}{P(X=x_i)}\right)$  is defined as the aggregator's information gain.

From the definition 3 above, we can measure the amount of uncertainty reduction about real data after the aggregator has observed the disguised data. In fact, such metrics is a comparison between the prior and posterior probability of the real data. What's more, we noticed that this metrics has the same form with the well-known MI in information theory. Furthermore, the expected MI measures the information of a user loses on average, which can be used to measure information leakage of a privacy mechanism, i.e., MI leakage. Based on the notion of MI leakage, we argue that the equivalent  $\epsilon$ -privacy mechanisms is comparable with each other. To demonstrate a partially ordered relation, we give the following definition.

**Definition 4:** For a given prior probability distribution  $P$ , and arbitrary two privacy mechanisms  $Q^i, Q^j \in \mathcal{Q}$  (s.t.  $1 \leq i, j \leq k$ ), if  $I(P; Q^i) \leq I(P; Q^j)$ , then  $Q^i \succeq Q^j$ , otherwise  $Q^i \prec Q^j$ .

More especially this relation is transitive, and it can be used to compare the privacy protection intensity of different mechanisms. Next, we consider the meaning of MI for privacy-preserving mechanism. First, the MI measures privacy leakage, which focus on the uncertainty of the real data given the disguised data. Second, the disguised data should preserve the information content of real data as much as possible while meeting the LDP constraints. Further, the information content in disguised data about real data is measured by the well-known MI [7]. Based on these theoretical supports, we consider the rational user aims to decrease the MI between real data and disguised data so that the aggregator can not have enough information to complete identify a user's personal data. However, the rational aggregator wants to maximize the privacy leakage to get more private information. From the analysis above, we can formulate the objective of users as the following *minimax problem*, such as

$$\inf_{Q \in \mathcal{Q}} \sup_{P \in \mathcal{P}} I(P; Q). \quad (7)$$

In addition, the aggregator will estimate a distribution that maximizes MI because the set of prior distribution is available for him. In this case, the worst-case MI leakage of any privacy mechanism will be

$$\sup_{P \in \mathcal{P}} \inf_{Q \in \mathcal{Q}} I(P; Q). \quad (8)$$

In fact, the above problem is formulated as a minimax problem, which becomes an convex optimization problem [44]. The minimax problem captures a basic scenario, where the players' goals are just opposite. In practice, the aggregator may be an strategic player rather than limited to observing the disguised data, who can change his own strategy according to the user's protection strategy. In such case, we consider MI leakage as the gain of the aggregator.

## V. GAME MODEL AND ANALYSIS

In this section, we formulate the minimax privacy problem as a two-person zero-sum game, and further provide the theoretic analysis.

### A. PRIVACY-PRESERVING ATTACK AND DEFENCE GAME MODEL

Each user perturbs her real data using privacy-preserving mechanism, who is analogous to a *defender*. As such, the aggregator is analogous to an *attacker*. Analogy-based, the above minimax problem naturally evolves into an attack and defence game problem. To have a better presentation, we first provide a formal definition.

**Definition 5:** The privacy-preserving attack and defense (PPAD) game-theoretic framework is a tuple  $(D, A, \mathcal{D}, \mathcal{A}, U)$ , where  $\mathcal{D}$  and  $\mathcal{A}$  are the strategic space of the privacy

defender  $D$  and attacker  $A$  respectively, and  $U : \mathcal{D} \times \mathcal{A} \rightarrow \mathbb{R}$  is a *von Neumann-Morgenstern utility function*. Then, the rational behaviors both for them can be defined as

$$\begin{cases} s_d^* \stackrel{\text{def}}{=} \arg \min_{s_d \in \mathcal{D}} U_D(s_d, s_a^*) \\ s_a^* \stackrel{\text{def}}{=} \arg \max_{s_a \in \mathcal{A}} U_A(s_d^*, s_a). \end{cases} \quad (9)$$

In the above definition 5, we present a standard description about the PPAD game. To explain in details, we provide the game description of our PPAD, including players, strategic space and payment. Firstly, the players of PPAD game are attacker and defender. Secondly, the defender aims to decrease the private information loss, i.e., the desired information gain of attacker. Thus, we define a set of privacy mechanisms as the strategic space of the defender, denoted as  $\mathcal{D} \triangleq \mathcal{Q}$ . Besides, we define all of possible distributions  $\mathcal{P}$  on  $\mathcal{X}$  as attacker's strategic space, denoted as  $\mathcal{A} \triangleq \mathcal{P}$ . Thirdly, we define MI as the payoff function. To be specific, for any  $P \in \mathcal{P}$  and  $Q \in \mathcal{Q}$ , the payment is calculated by

$$U(P, Q) = \sum_{\mathcal{X}} \sum_{\mathcal{Y}} P^T Q \log \left( \frac{Q}{\sum_{\mathcal{X}} P^T Q} \right) \quad (10)$$

In the above PPAD game, the private information loss of the defender is the gaining of the attacker, which means that the goal of the defender is to minimize the loss, while the attacker aims to maximize the payment. Thus, the proposed PPAD is a two-person zero-sum (TPZS) game. We make a remark regarding the proposed game model. The saddle point strategy of PPAD game also provides a certain level of differential privacy. This is because the available actions of the defender are  $\epsilon$ -privacy mechanisms. Hence, PPAD guarantees certain level of differential privacy, and  $\epsilon$  is determined by the saddle point strategy. To have a better illustration of our idea, we provide an example.

**Example 2:** Assume the set of source distribution  $\mathcal{P}$  contains 3 different distributions on source alphabet with  $|\mathcal{X}| = 3$ , denoted as  $P^i \in \mathcal{P}, i \in \{1, 2, 3\}$ . The instances are given in Table 2.

**TABLE 2. The prior probability distributions.**

	$P_{(1)}$	$P_{(2)}$	$P_{(3)}$
$P^1$	0.25	0.35	0.4
$P^2$	0.35	0.5	0.15
$P^3$	0.6	0.2	0.2

Moreover, we consider that the set of privacy mechanisms  $\mathcal{Q}$  also includes 3 different mechanisms, denoted as  $\mathcal{Q} = \{Q^1, Q^2, Q^3\}$ . Table 3 shows them in details. As such, the above PPAD game is an instance of matrix games.

In this paper, we consider a simultaneous game with perfect information, which means that each player makes a decision without knowing the decision made by the other. In the PPAD game, we consider that the players' strategic actions and payoff function are common knowledge that they are known both by the attacker and the defender. In this case, we analyze the rational actions for the players of PPAD game. In fact,

**TABLE 3.**  $\epsilon = \ln 2$  privacy mechanisms.

$\mathcal{Q}$	$Q_{(y x)}^1$			$Q_{(y x)}^2$			$Q_{(y x)}^3$		
	1	2	3	1	2	3	1	2	3
1	0.4	0.3	0.3	0.4	0.2	0.4	0.3	0.2	0.5
2	0.25	0.15	0.6	0.3	0.3	0.4	0.2	0.4	0.4
3	0.2	0.2	0.6	0.2	0.4	0.4	0.15	0.35	0.5

a solution of the strategic game is captured by the saddle point. In the following, we provide the theoretic analysis for the proposed PPAD game.

### B. CONVEX-CONCAVE ANALYSIS

The well-known convex-concave game has a special form that the payoff function is a convex function of one player's actions, and it is a concave function of the other's actions [45]. In such games, the solutions are given by the pure strategies for each player.

For our PPAD game model, the strategies of attacker and defender are probabilistic sets, that is, they are convex sets. Therefore, for any convex combination of  $P^1, P^2 \in \mathcal{P}$ , the  $U(P)$  satisfies a concave function of a closed convex set. In addition, for any  $Q^1, Q^2 \in \mathcal{Q}$ , and a parameter  $\lambda \in \mathbb{R}^+, 0 < \lambda < 1$ , then their convex combination  $Q^\lambda = \lambda Q^1 + (1 - \lambda)Q^2$  also satisfies  $\epsilon$ -differential privacy, which has been proved in [13]. As a result, for each  $P$ , the payoff function is a convex function of  $Q$ . Based on these theoretic analysis, the game that we proposed in this paper is a *convex-concave game*.

**Lemma 1:** If  $U : \mathcal{P} \times \mathcal{Q} \rightarrow \mathbb{R}$  is a concave function of  $P$ , then attacker has an optimal response strategy such that  $\max_{P \in \mathcal{P}} \min_{Q \in \mathcal{Q}} U(P, Q)$ . Similarly, if it is a convex function of  $Q$ , then the defender has an optimal response strategy such that  $\min_{Q \in \mathcal{Q}} \max_{P \in \mathcal{P}} U(P, Q)$ .

The proof of Lemma 1 is similar to the proof of Theorem 5.2 in [45], thus we omit this proof for space limitation.

In addition to the mentioned above, we noticed that the PPAD game is a simultaneous game with complete information, thus each player can predict other's optimal response strategy, i.e. dominant strategy. As a result, no matter an attacker or defender will have an optimal response strategy for the other's strategy. Based on this result, we have the following Theorem 2.

**Theorem 2:** For finite probability sets  $\mathcal{P}$  and  $\mathcal{Q}$ , the privacy-preserving attack and defense, PPAD game exists a saddle-point  $(P^*, Q^*)$  satisfying  $U(P, Q^*) \leq U(P^*, Q^*) \leq U(P^*, Q)$  for  $\forall P \in \mathcal{P}$  and  $\forall Q \in \mathcal{Q}$ .

**Proof:** For arbitrary  $Q^1, Q^2 \in \mathcal{Q}$ , and a parameter  $\lambda \in \mathbb{R}^+ (0 < \lambda < 1)$ , their convex combination  $Q^\lambda = \lambda Q^1 + (1 - \lambda)Q^2$  is also a  $\epsilon$ -LDP [13]. Because that both  $\mathcal{P}$  and  $\mathcal{Q}$  are probability distribution sets, thus they are convex subset of Euclidean space. Furthermore,  $U(P, Q)$  is a function of two variables, which is concave in  $P$  for each  $Q$  and convex in  $Q$  for each  $P$  [42]. What's more, the finite sets of  $\mathcal{P}$  and  $\mathcal{Q}$  are compact, i.e. closed and bounded. Then, according to the well-known minimax theorem, the PPAD game exists a saddle-point.

From the Theorem 2 above, we can see that the saddle-point of proposed PPAD game is an extremal status of privacy leakage, which is the worst-case for privacy defender. In addition, Equation (6) indicates that the payment of saddle-point is the minimum information gain that an attacker can obtain from the real data. At the same time, this payment is the defender's maximum possible information loss. Therefore, the saddle point of PPAD can be used to assess mutual information (MI) leakage. Indeed, the corresponding payment is an upper bound of MI leakage.

### C. GAME ANALYSIS

Game analysis aims to find the solutions of games, which is one of the major research objectives in the game theory. It is well-known that the solution of game is a steady state that each player has no incentive to deviate from this state, i.e., no player wants to change his current strategy. Based on the above Lemma 1, the strategy profile of saddle point needs to be the optimal response strategy that both for each player. In fact, the proposed PPAD game is a TPZS game with finite strategies. From the Theorem 2, our PPAD game has a saddle point because the convexity and concavity of the payoff function. In calculating the saddle point, the calculation is an iterative optimization problem between two convex sets. Inspired by this idea, we propose an algorithm to calculate the solution of the established PPAD game.

The procedures of solving maximin problem is an alternating optimization, and it is similar to the problem of minimizing distance between two convex sets. The basic idea is alternate to calculate an optimal response strategy between two convex sets, which mainly includes three steps:

---

#### Algorithm 1 Optimal Response Strategy for PPAD Game

##### Input:

Strategic actions  $\mathcal{P}, \mathcal{Q}$  and payoff function  $U(P, Q)$

##### Output:

Saddle point  $(P^*, Q^*)$  and its payment SD

- 1: Initialize set  $S_1 \leftarrow Q^0$  with an arbitrary  $Q^0 \in \mathcal{Q}$
  - 2: Calculate  $P^*$  via Equation (8)
  - 3: Calculate  $Q^*$  by Equation (7)
  - 4: **while**  $(P^*, Q^*)$  is not a saddle point **do**
  - 5:     Calculate  $P^*$  via Equation (8), and update  $P^*$  to recalculate  $U(P^*, Q^*)$  by Equation (10)
  - 6:     **if**  $(P^*, Q^*)$  is saddle point **then**
  - 7:         **return**  $(P^*, Q^*)$  and  $SD \leftarrow U(P^*, Q^*)$
  - 8:     **else**
  - 9:         Calculate  $Q^* = \arg \min_{Q \in \mathcal{Q} \setminus S_1} U(P^*, Q)$ , and  $U(P^*, Q^*)$  by Equation (10)
  - 10:         Update set  $S_1 \leftarrow S_1 \cup Q^*$
  - 11:     **end if**
  - 12: **end while**
- 

**Step 1:** For a single arbitrary strategy of defender, the attacker calculates an optimal response strategy satisfying  $\arg \max_{P \in \mathcal{P}} U(P, Q)$ ;

**Step 2:** Further, the defender predicts the attacker's preference, thus the defender would like to take the action that satisfies  $\arg \min_{Q \in \mathcal{Q}} \max_{P \in \mathcal{P}} U(P, Q)$ ;

**Step 3:** Finally, alternating procedure updates their strategy choices, and repeats the above steps until a strategy profile  $(P^*, Q^*)$  that is optimal both for the attacker and defender.

Next, we present these calculation procedures in a algorithm, and provide the description in details.

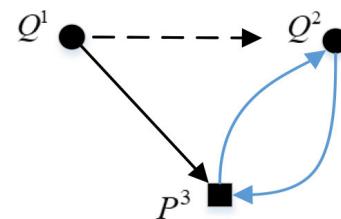
The Algorithm 1 receives the structure of PPAD game, including strategic spaces  $\mathcal{P}$  and  $\mathcal{Q}$  and payoff function  $U(P, Q)$ . Then, it performs the calculations to output the saddle point and payment. Firstly, it initializes an arbitrary strategy  $Q^0 \in \mathcal{Q}$ , and calculates an optimal response strategy for  $Q^0$  by using Equation (8) (lines 1 ~ 2 of Algorithm 1). Secondly, it calculates an optimal response strategy of defender by Equation (7), which is used to defend attacker's strategy (line 3 of Algorithm 1). Thirdly, it repeats these procedures of alternating optimization until a stable state  $(P^*, Q^*)$  that are both optimal for the attacker and defender (lines 4 ~ 13 of Algorithm 1). Finally, it returns the saddle point and corresponding payment.

To understand our algorithm intuitively, we provide the explanation using Example 2 and illustrate the payments in Table 4. We demonstrate these procedures by assuming the algorithm begins with the strategy  $Q^1$ , then, the attacker prefers to take  $P^3$  for the purpose to obtain a maximum payment 0.0662, i.e.,  $P^3$  is an optimal strategy for the attacker. Further, the defender predicts the attacker's action, and takes  $Q^2$  to minimize the privacy loss. That is to say, the defender desires to achieve 0.0315, thus  $Q^2$  is the defender's optimal strategy to defend  $P^3$ . Meanwhile,  $P^3$  is also the optimal strategy for defender's strategy  $Q^2$ . Therefore, the strategy profile  $(P^3, Q^2)$  is a saddle point of the PPAD game, which has a payment 0.0315. Also, the saddle point strategy guarantees  $\epsilon = \ln 2$  differential privacy. Additionally, we depict the procedures of rational decision in Figure 2 to have a better illustration.

**TABLE 4.** The payments of Example 2.

	$Q^1$	$Q^2$	$Q^3$	
$P^1$	0.0531	0.0308	0.0299	.0299
$P^2$	0.0627	0.0226	0.0339	.0226
$P^3$	0.0662	0.0315	0.0345	.0315
	.0662	.0315	.0345	

We provide the computation complexity of Algorithm 1 by analyzing some fundamental operations. First, the attacker's strategic space  $\mathcal{P}$  is searched to find an optimal response strategy  $P$  in the first iteration. Second, the algorithm calculates the optimal reaction  $Q$  to the attacker's strategy, which searches the strategic space of the defender. Finally, the termination condition guarantees the solution of maxmin problem. It is clear then that the cost grows with the sizes of  $\mathcal{P}$  and  $\mathcal{Q}$ .



**FIGURE 2.** Illustration of the rational decision.

As long as both  $\mathcal{P}$  and  $\mathcal{Q}$  are finite, the whole procedures will be efficient.

## VI. EXPERIMENTAL SIMULATIONS AND ANALYSIS

In this section, we illustrate the experimental results of our scheme, and further provide the analytic results. We implement the algorithm in Java and conduct our experiments on a PC running Win 10 OS.

### A. CASE STUDY

For the case of  $|\mathcal{X}| = |\mathcal{Y}| = 6$ , we assume that the prior probability distribution lies in a certain set but does not know the true distribution exactly. To have an illustration intuitively, we borrow several distributions from [13], and show them in Table 5.

**TABLE 5.** The possible probability distributions.

	$P(1)$	$P(2)$	$P(3)$	$P(4)$	$P(5)$	$P(6)$
$P^1$	0.7	0.15	0.06	0.04	0.03	0.02
$P^2$	0.15	0.7	0.06	0.04	0.03	0.02
$P^3$	0.06	0.15	0.7	0.04	0.03	0.02
$P^4$	0.04	0.15	0.06	0.7	0.03	0.02

Furthermore, we consider two alternative privacy mechanisms with  $\epsilon = \ln 2$ . Their probability density functions are shown in Table 6, where  $Q^1$  is the truncated  $\frac{1}{2}$ -geometric mechanism [46] and  $Q^2$  is a privacy mechanism that proposed in [23]. Further, we consider the well-known  $k$ -RR mechanism [7] that its diagonal probabilities are  $e^\epsilon / (|\mathcal{X}| - 1 + e^\epsilon)$ . The  $k$ -RR provides  $\epsilon = \ln 2$  differential privacy guarantee, if and only if its probability density function  $Q^3$  satisfies

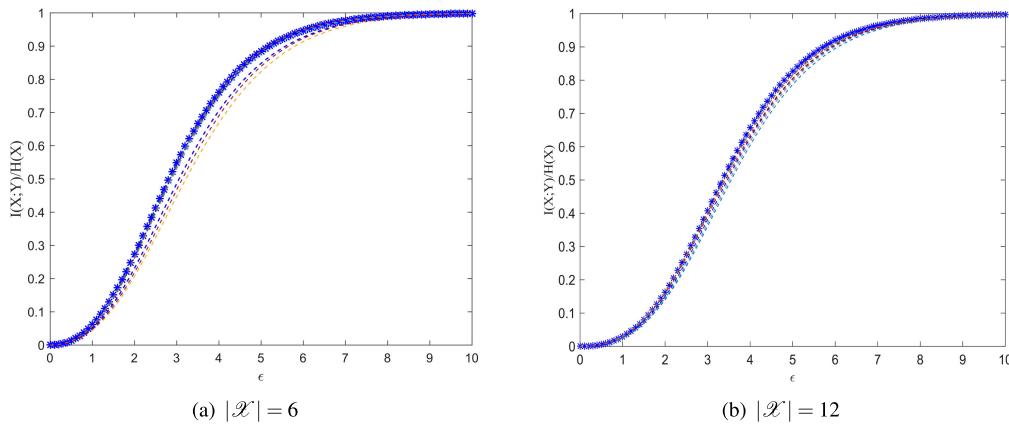
$$Q_{(y|x)}^3 = \begin{cases} \frac{e^\epsilon}{|\mathcal{X}| - 1 + e^\epsilon} & y = x, \\ \frac{1}{|\mathcal{X}| - 1 + e^\epsilon} & y \neq x. \end{cases} \Rightarrow Q_{(y|x)}^3 = \begin{cases} 2/7 & y = x, \\ 1/7 & y \neq x. \end{cases}$$

We noticed that the mechanisms of  $\{Q^1, Q^2, Q^3\}$  are equivalent  $\ln 2$ -privacy mechanisms. To compare these privacy mechanisms, we assume they are possible privacy strategies of the privacy defender. In this case, we provide the analytic result below.

Based on these available actions, we analyze the rational behaviors of the attacker and defender. The corresponding game is solved by Algorithm 1. As a result, the algorithm outputs a saddle point  $(P^1, Q^3)$  and payment 0.0351, which

**TABLE 6.**  $\epsilon = \ln 2$  alternative privacy mechanisms with  $|\mathcal{X}| = 6$ .

In/Out	$Q_{(y x)}^1$						$Q_{(y x)}^2$					
	1	2	3	4	5	6	1	2	3	4	5	6
1	2/3	1/6	1/12	1/24	1/48	1/48	4/11	2/11	1/11	1/11	1/11	2/11
2	1/3	1/3	1/6	1/12	1/24	1/24	2/11	4/11	2/11	1/11	1/11	1/11
3	1/6	1/6	1/3	1/6	1/12	1/12	1/11	2/11	4/11	2/11	1/11	1/11
4	1/12	1/12	1/6	1/3	1/6	1/6	1/11	1/11	2/11	4/11	2/11	1/11
5	1/24	1/24	1/12	1/6	1/3	1/3	1/11	1/11	1/11	2/11	4/11	2/11
6	1/48	1/48	1/24	1/12	1/6	2/3	2/11	1/11	1/11	1/11	2/11	4/11



**FIGURE 3.** The normalized  $I(X; Y)/H(X)$  of privacy mechanisms for randomly generated 10 distributions.

means the MI privacy leakage would not exceed an upper bound (0.0351). In other cases, the defender has an incentive to change his current strategy. For instance, when we consider the uniform prior distribution, the payment of game will be 0.0633. In summary, these results indicate that the optimal privacy preserving mechanism is related to the prior distribution.

What's more, we solve the problem that not being able to compare between equivalent privacy preserving mechanisms by using the information-theoretic approach. For instance, taking the uniform prior distribution into consideration, MI privacy leakage of these mechanisms are in fact strict orderings, i.e.  $Q^1 = 0.5074 > Q^2 = 0.2164 > Q^3 = 0.0633$ . In fact, these numbers of MI leakage describe the defender's preference for different outcomes. Thus, we have  $Q^3 > Q^2 > Q^1$ . This strict ordering provides an effective evaluation method for equivalent  $\epsilon$ -privacy mechanisms.

## B. NUMERICAL SIMULATION

In order to obtain the numerical simulation results, we randomly generate 10 different distributions for  $|\mathcal{X}| = 6$  and  $|\mathcal{X}| = 12$ , respectively. Then, we use the randomized response to implement the privacy-preserving mechanism. Following [7], we set  $\epsilon$  ranging from 0 to 10 that we can obtain a set of privacy mechanisms. Based on these simulation data, we provide the following analysis.

We assume that the distributions (resp. mechanisms) are available actions of the attacker (resp. defender). Further, we conduct the experiment on these generated data, and

perform Algorithm 1 to calculate the saddle point of PPAD game. To overcome the effect of randomness, we compare the average performance measured by the normalized mutual information  $I(X; Y)/H(X)$  for all privacy mechanisms, i.e. privacy payment. In our PPAD game, the rational privacy attacker (resp. defender) prefers to take the strategy that maximizes (resp. minimizes) the outcome of game. In fact, MI privacy leakage is monotonicity about  $\epsilon$ , thus the curve of normalized mutual information can be drawn with  $\epsilon$  increasing.

The experimental results are shown in Figure 3. We can see that the MI privacy leakage of saddle point is the worst-case privacy leakage for privacy defender. Besides, Figure 3(a) and Figure 3(b) are confirm that the conclusion is not sensitive to the size of  $|\mathcal{X}|$  because two experimental results have the same tendency. This worst-case MI leakage can help to assess privacy disclosure risks and choose the adaptive  $\epsilon$  under the tolerable breach of privacy.

## VII. CONCLUSION AND FUTURE WORK

In this work, we have formalized the problem of trade-off between privacy and utility as a minimax problem, and proposed the PPAD game-theoretic framework using information-theoretic approach. In particular, the established PPAD game is a TPZS game. To find the solution, we proposed an alternating optimization algorithm to compute the saddle point. Then, we demonstrated our scheme that can be used to compare the performance between equivalent privacy mechanisms. Further, we illustrated our privacy measure is

the worst-case privacy leakage, that is, maximum privacy leakage for privacy defender.

In the future work, there still exists several interesting questions that are worthy to be further investigated. For example, the defender first takes action, and then the attacker takes action after observing the defender's action, thus the game model will evolve into a Steinberg game or dynamic game model of incomplete information. Moreover, all participants are assumed to be rational players to investigate the privacy-preserving mechanism design, which is also a fascinating topic.

## REFERENCES

- [1] C. Dwork, "Differential privacy," in *Proc. 33rd Int. Conf. Automata, Lang. Program. (ICALP)*, vol. 2, 2006, pp. 1–12.
- [2] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Proc. 3rd Conf. Theory Cryptogr. (TCC)*, vol. 3876, 2006, pp. 265–284.
- [3] J. Duchi, M. J. Wainwright, and M. I. Jordan, "Local privacy and minimax bounds: Sharp rates for probability estimation," in *Proc. Adv. Neural Inf. Process. Syst.*, 2013, pp. 1529–1537.
- [4] S. L. Warner, "Randomized response: A survey technique for eliminating evasive answer bias," *J. Amer. Stat. Assoc.*, vol. 60, no. 309, pp. 63–69, 1965.
- [5] Ú. Erlingsson, V. Pihur, and A. Korolova, "RAPPOR: Randomized aggregatable privacy-preserving ordinal response," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2014, pp. 1054–1067.
- [6] G. Fanti, V. Pihur, and Ú. Erlingsson, "Building a RAPPOR with the unknown: Privacy-preserving learning of associations and data dictionaries," *Proc. Privacy Enhancing Technol.*, vol. 2016, no. 3, pp. 41–61, Jul. 2016.
- [7] P. Kairouz, S. Oh, and P. Viswanath, "Extremal mechanisms for local differential privacy," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 4, 2014, pp. 2879–2887.
- [8] J. Tang, A. Korolova, X. Bai, X. Wang, and X. Wang, "Privacy loss in Apple's implementation of differential privacy on MacOS 10.12," 2017, *arXiv:1709.02753*. [Online]. Available: <http://arxiv.org/abs/1709.02753>
- [9] P. Kairouz, K. Bonawitz, and D. Ramage, "Discrete distribution estimation under local privacy," in *Proc. 33rd Int. Conf. Int. Conf. Mach. Learn. (ICML)*, vol. 48, 2016, pp. 2436–2444.
- [10] Y. Wang, X. Wu, and D. Hu, "Using randomized response for differential privacy preserving data collection," in *Proc. EDBT/ICDT Workshops*, 2016. [Online]. Available: <http://ceur-ws.org/Vol-1558/paper35.pdf>
- [11] N. Holohan, D. J. Leith, and O. Mason, "Optimal differentially private mechanisms for randomised response," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2726–2735, Nov. 2017.
- [12] S. Xiong, A. D. Sarwate, and N. B. Mandayam, "Randomized requantization with local differential privacy," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Mar. 2016, pp. 2189–2193.
- [13] K. Kalantari, L. Sankar, and A. D. Sarwate, "Robust privacy-utility trade-offs under differential privacy and Hamming distortion," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2816–2830, Nov. 2018.
- [14] M. Lopuhä-Zwakenberg, B. Škorić, and N. Li, "Information-theoretic metrics for local differential privacy protocols," 2019, *arXiv:1910.07826*. [Online]. Available: <http://arxiv.org/abs/1910.07826>
- [15] F. du Pin Calmon and N. Fawaz, "Privacy against statistical inference," in *Proc. 50th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2012, pp. 1401–1408.
- [16] A. D. Sarwate and L. Sankar, "A rate-distortion perspective on local differential privacy," in *Proc. 52nd Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2014, pp. 903–908.
- [17] K. Kalantari, L. Sankar, and A. D. Sarwate, "Optimal differential privacy mechanisms under Hamming distortion for structured source classes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 2069–2073.
- [18] W. Wang, L. Ying, and J. Zhang, "On the relation between identifiability, differential privacy, and mutual-information privacy," *IEEE Trans. Inf. Theory*, vol. 62, no. 9, pp. 5018–5029, Sep. 2016.
- [19] D. J. Mir, "Information-theoretic foundations of differential privacy," in *Proc. 5th Int. Conf. Found. Pract. Secur. (FPS)*, 2012, pp. 374–381.
- [20] T. Wang, M. Lopuhä-Zwakenberg, Z. Li, B. Skoric, and N. Li, "Locally differentially private frequency estimation with consistency," 2019, *arXiv:1905.08320*. [Online]. Available: <http://arxiv.org/abs/1905.08320>
- [21] C. Dwork, "Differential privacy: A survey of results," in *Proc. 5th Int. Conf. Theory Appl. Models Comput. (TAMC)*, vol. 4978, 2008, pp. 1–19.
- [22] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, nos. 3–4, pp. 211–407, 2014.
- [23] M. S. Alvim, M. E. Andrés, K. Chatzikokolakis, P. Degano, and C. Palamidessi, "Differential privacy: On the trade-off between utility and information leakage," in *Proc. Formal Aspects Secur. Trust*, vol. 7140, 2011, pp. 39–54.
- [24] M. S. Alvim and M. E. Andrés, "On the relation between differential privacy and quantitative information flow," in *Proc. Int. Colloq. Automata Lang. Program.*, vol. 6756, 2011, pp. 60–76.
- [25] M. Min, X. Wan, L. Xiao, Y. Chen, M. Xia, D. Wu, and H. Dai, "Learning-based privacy-aware offloading for healthcare IoT with energy harvesting," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4307–4316, Jun. 2019.
- [26] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "Utility-privacy tradeoffs in databases: An information-theoretic approach," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 838–852, Jun. 2013.
- [27] G. Barthe and B. Kopf, "Information-theoretic bounds for differentially private mechanisms," in *Proc. IEEE 24th Comput. Secur. Found. Symp.*, Jun. 2011, pp. 191–204.
- [28] P. Cuff and L. Yu, "Differential privacy as a mutual information constraint," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 43–54.
- [29] A. Makhdoumi and N. Fawaz, "Privacy-utility tradeoff under statistical uncertainty," in *Proc. 51st Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2013, pp. 1627–1634.
- [30] T. Murakami and Y. Kawamoto, "Utility-optimized local differential privacy mechanisms for distribution estimation," in *Proc. 28th USENIX Secur. Symp. (USENIX Secur.)*, 2019, pp. 1877–1894.
- [31] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *Proc. 48th Annu. IEEE Symp. Found. Comput. Sci. (FOCS)*, Oct. 2007, pp. 94–103.
- [32] Y. Tian, Z. Wang, J. Xiong, and J. Ma, "A blockchain-based secure key management scheme with trustworthiness in DWSNs," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 6193–6202, Sep. 2020.
- [33] C. Zerui, Y. Tian, and C. Peng, "An incentive-compatible rational secret sharing scheme using blockchain and smart contract," *Sci. China Inf. Sci.*, 2020. [Online]. Available: <http://engine.scichina.com/doi/10.1007/s11432-019-2858-8>; doi: [10.1007/s11432-019-2858-8](https://doi.org/10.1007/s11432-019-2858-8).
- [34] Y. Xiao, L. Xiao, X. Lu, H. Zhang, S. Yu, and H. V. Poor, "Deep reinforcement learning based user profile perturbation for privacy aware recommendation," *IEEE Internet Things J.*, early access, Sep. 29, 2020, doi: [10.1109/IJOT.2020.3027586](https://doi.org/10.1109/IJOT.2020.3027586).
- [35] J. Hsu, A. Roth, and J. Ullman, "Differential privacy for the analyst via private equilibrium computation," in *Proc. 45th Annu. ACM Symp. Symp. Theory Comput.*, 2013, pp. 341–350.
- [36] M. S. Alvim, K. Chatzikokolakis, Y. Kawamoto, and C. Palamidessi, "Information leakage games," *Decis. Game Theory Secur.*, vol. 10575, pp. 437–457, Oct. 2017.
- [37] M. S. Alvim, K. Chatzikokolakis, Y. Kawamoto, and C. Palamidessi, "Leakage and protocol composition in a game-theoretic perspective," in *Proc. Princ. Secur. Trust*, 2018, pp. 134–159.
- [38] R. Jin, X. He, and H. Dai, "On the security-privacy tradeoff in collaborative security: A quantitative information flow game perspective," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 12, pp. 3273–3286, Dec. 2019.
- [39] H. Gao, H. Xu, L. Zhang, and X. Zhou, "A differential game model for data utility and privacy-preserving in mobile crowdsensing," *IEEE Access*, vol. 7, pp. 128526–128533, 2019.
- [40] F. Fioretto, L. Mitridati, and P. Van Hentenryck, "Differential privacy for stackelberg games," in *Proc. 29th Int. Joint Conf. Artif. Intell.*, 2020, pp. 3480–3486.
- [41] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, 1948.
- [42] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ, USA: Wiley, 2006.
- [43] T. Barna, J. Von Neumann, and O. Morgenstern, "Theory of games and economic behaviour," *Economica*, vol. 107, no. 50, p. 136, 1944.
- [44] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York, NY, USA: Cambridge Univ. Press, 2004.
- [45] A. R. Washburn, *Two-Person Zero-Sum Games*, 4th ed. New York, NY, USA: Springer, 2014.
- [46] A. Ghosh, T. Roughgarden, and M. Sundararajan, "Universally utility-maximizing privacy mechanisms," *SIAM J. Comput.*, vol. 41, no. 6, pp. 1673–1693, Jan. 2012.



**NINGBO WU** received the M.S. degree from the School of Information, Guizhou University of Finance and Economics, China, in 2016. He is currently pursuing the Ph.D. degree with the College of Computer Science and Technology, Guizhou University, China. He is also a Scholar with the State Key Laboratory of Public Big Data. His research interests include privacy preserving, data security, coding and information theory, and game theory.



**KUN NIU** received the B.S. and M.S. degrees from the China University of Mining and Technology, in 2008 and 2011, respectively. She is currently pursuing the Ph.D. degree with the College of Computer Science and Technology, Guizhou University, China. Her research interests include big data security, privacy computing, and privacy protection.

• • •



**CHANGGEN PENG** received the Ph.D. degree from the College of Computer Science and Technology, Guizhou University, China, in 2007. He is currently a Professor and a Ph.D. Supervisor with the College of Computer Science and Technology, Guizhou University. He is also an Academic Leader of data security and cryptography with the State Key Laboratory of Public Big Data. His research interests include data privacy, cryptography, and big data technology and security.