Information-Theoretic Approaches to Differential Privacy

Ayşe Ünsal Melek Önen

EURECOM, France
firstname.lastname@eurecom.fr

Abstract

This tutorial studies relationships between differential privacy and various information-theoretic measures by using several selective articles. In particular, we present how these connections can provide new interpretations for the privacy guarantee in systems that deploy differential privacy in an information-theoretic framework. To this end, the tutorial provides an extensive summary on the existing literature that makes use of information-theoretic measures and tools such as mutual information, min-entropy, Kullback-Leibler divergence and rate-distortion function for quantification and characterization of differential privacy in various settings.

Index terms— differential privacy, mutual information, relative entropy, rate-distortion theory, min-entropy, leakage

1 Introduction

Over the past decade, machine learning (ML) algorithms have found application in a vast and rapidly growing number of systems for analysing and classifying large amounts of data. Despite the improvement and comfort that was brought to our daily lives by applications that employ these algorithms, they also gave cause for concern in terms of security and data privacy due to their undesired consequences. The increasing popularity of ML techniques opened the door for attackers, especially when these techniques were deployed to be used in critical areas as intrusion detection, autonomous driving or healthcare. In particular, an adversary may look for means to modify the model, misclassify some inputs and consequently succeed in unauthorized cyber-access, car accidents or even health problems. It is not unrealistic to imagine the scenario, where a self-driving car causes an accident due to ignoring a stop sign, which through tampering by an adversary was made to look like a parking sign.

In addition to the security aspect of such an attack, user-data privacy is also prone to violations in this problem. Such data is considered as highly sensitive, since it contains information on location that could lead to discovery of personal habits and may enable vehicle identification. In general, the high quality and high accuracy of ML predictions strongly depend on the collection of large datasets. Such a large-scale data collection gives cause for privacy concerns and makes users vulnerable to fraudulent use of personal information. When individuals willingly share some of their personal data with an Internet service, statistical independence of the representation of the data and the actual individual is a desired quality of the underlying system. At least from a conceptual perspective, a measure of this independence relates to the amount of privacy an individual can expect from the system. However, it is possible to successfully de-anonymize or re-identify the owner of the data as proven by a number of studies as follows [1–4]. For instance, Facebook and Cambridge Analytica are real-life examples of massively used online services, which were proven to be a threat to privacy of individuals back in 2010, when Cambridge Analytica acquired a great number of Facebook users' data for the purpose of using the right political advertisement. More recently, it was discovered that Pegasus spyware has been used for reading text messages, tracking calls and locations, accessing the targeted device's camera and microphone in many versions of Apple's iOS and Android [5]. These few examples of privacy rights' violations make it clear that protecting privacy of personal data is a major concern in today's world.

In order to address data privacy requirements in such contexts, two application methods are used in current systems, namely local and global privacy. In local privacy methods, individuals publish private version of their own information, as is the case of a social networking website. Global privacy methods make use of a trusted (central) server or curator which publishes private query responses related to a group of individuals. A common characteristic of both approaches is that data is typically coded using some randomizing function prior to its publication. Differential privacy [6] is a stochastic measure of privacy which is now used in conjunction with ML algorithms while managing large datasets to ensure data privacy of individual users. It has furthermore been used to develop practical methods for protecting private user-data when they provide information to the ML system. In these cases, the use of a differential privacy measure aims to preserve the accuracy of the ML model without incurring a cost of the privacy of individual participants. An embedded application in Google's Chrome Web Browser [7], a Census Bureau project called OntheMAP [8], LinkedIn and Apple's iOS 11 are only a few examples of real-life applications which have already deployed differential privacy to address and overcome this vulnerability of users in terms of privacy of personal information.

A mechanism or a randomized function of a dataset is called *differentially private* if the absence or presence of any participant's data has a negligible impact on the output of the mechanism when any of the participants decides to submit or equivalently remove their data from a statistical dataset. This idea is roughly depicted in Figure 1. In some sense, differential privacy is a notion of robustness against such changes in the dataset. The degree of this change is measured and determined by an adjustable privacy parameter (or the privacy budget) and the amount of the change that any single argument to the system reflects on its output is called the sensitivity of the system. The major challenge is to offset the accuracy of the output of a statistical dataset against the level of the privacy protection guaranteed to the participants. Indeed, noisier data results in a stronger level of privacy due to increased randomness and this reflects as a reduction in accuracy of the output.

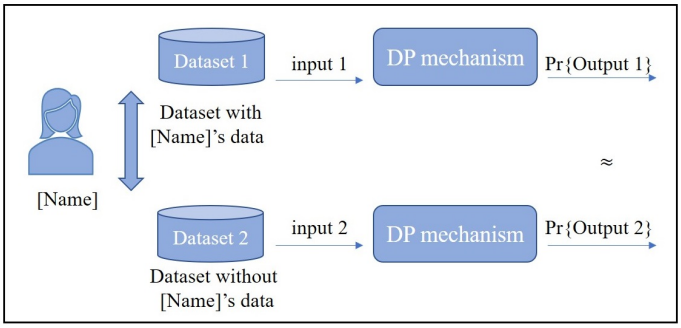

Figure 1: Differential privacy

Timeliness and necessity of the tutorial: Differential privacy arises a great interest among researchers particularly from computer science and statistics circles who contributed to what we already know about this strong mathematical formulation of privacy. There are several detailed surveys of what is known today regarding differential privacy from the perspective of computer scientists and statisticians [9–11]. More recently, also researchers in information theory/electrical engineering circles contributed to the literature on the subject. However, a full information-theoretic understanding of differential privacy and its information-theoretic connections with other trustworthy features are still lacking. This tutorial provides a *selective* summary of what we know regarding the relationship between differential privacy and information theory to enable information theorists, primarily, to build up on that to produce fundamental formulations and limits of privacy in various settings.

On the relevance of information-theoretic connections with differential privacy: Originally, the use of mutual information functional as privacy metric dates back to [12] for studying the domain of genome privacy prior to the existence of differential privacy. Even though there are different opinions on the form of the exact relation, a number of studies relate the (conditional [13] or unconditional [14,15]) mutual information between the entries of the dataset and the query response to differential privacy, which could be interpreted as a measure of utility as well as of privacy. Under certain conditions, differential privacy and the *mutual information differential privacy*, have proven to be equal in [13] where the authors redefine well-known information theoretic quantities as privacy constraint. Overall, a mutual information-based approach to differential privacy will allow many rules and properties that apply to the mutual information functional to be carried on to differential privacy leaving no room for ambiguity regarding the essence of the privacy guarantee. Furthermore, in [13], the mutual information-based differential privacy removes the requirement for neighborhood among datasets and strengthens the original definition. Hereafter, we enlist possible directions of research where the information-theoretic connections with differential privacy is pertinent. The reader should note that the following list is exemplary and non-exhaustive. Some items will be studied in detail within the content of this tutorial in further sections.

- **Cryptography:** A major example is the connection with *semantic security* via an information-theoretic approach. [16] proves an equivalence between a mutual information based differential privacy constraint and semantic security where a maximization is taken over database distributions. Additionally, [17] introduces a new data-privacy protection model that aims to achieve *Dalenius' goal* as well as to have better utility. The privacy channel capacity results are obtained through direct translations of well-known information theoretic approaches to differential privacy. In particular, the parallel drawn between the information privacy model and the multiple-access channel makes a great promise for the use of an information-theoretic framework to quantify the privacy guarantee that a differentially private system can provide to its users.

- **Security:** [18] presented an application of the so-called Kullback-Leibler differential privacy [13] (to be defined later) for detecting misclassification attacks in differentially private Laplace mechanisms. Accordingly, the corresponding distributions of relative entropy are considered as the differentially private noise with and without the adversary's advantage in order to establish the relationship between the impact of the attack and the detection of the adversary as a function of the sensitivity and the privacy budget of the mechanism. Besides adversarial classification, information-theoretic approaches for bounding the *communication complexity* of computing a function, which originally uses combinatorial measures [19] can also be applied to differential privacy. Information complexity [20] is a lower bound on communication complexity that is obtained using Shannon's mutual information and refers to the minimum amount of information that a communication protocol leaks about its users' inputs. [21] introduces an upper bound on the information cost of a two-party differentially private protocol using the same approach that will be studied in

detail in Section 4. [22], on the other hand covers, the privacy of physical layer for a two receiver broadcast channel through analyzing connections between a differential privacy based metric to physical layer secrecy. Accordingly, the authors show that for the privacy of anonymous communication networks in the case of a degraded two-user broadcast channel, differentially private receiver-message unlinkability is equivalent up to a constant to several secrecy metrics. Finally, [22] presents the rate region of the $(\epsilon, \delta)-$ differentially private receiver-message unlinkability satisfying strong secrecy.

- **ML:** Probably approximately correct (PAC) learning theory, which composes the mathematical framework of ML, is related to differentially private learning by using mutual information function in [23]. Accordingly, the author establishes an information-theoretic connection between Gibbs estimator which gives the minimum of PAC-Bayesian bounds and the exponential mechanisms to show that Gibbs estimator minimizes the expected empirical risk and the mutual information between the sample and the predictor.
- **Quantum computation:** There also has been a serious effort towards building connections between quantum computation and differential privacy [24–27]. Some works build the bridge between the two via *quantum information theory* that draws Shannon information theory, quantum mechanics and computer science together. Quantum differential privacy is originally defined in [26] for adaptation of differential privacy to quantum information processing. [24] focuses on quantum differential privacy using an information-theoretic framework, which is translated into quantum divergence.

Outline: Section 2 provides necessary preliminaries from the literature on differential privacy. Introductory preliminaries are followed by novel metrics derived through information-theoretic measures for quantifying privacy guarantee of differentially private mechanisms in Section 3 along with their ordering and comparisons. Section 4 presents upper bounds on information cost and maximal leakage based on Shannon entropy as well as min-entropy in differentially private mechanisms. In Section 5, we discuss the connections between differential privacy and source-coding theory, in addition to an exemplary result on adversarial classification in differentially private mechanisms from a rate-distortion perspective. To conclude, in Section 6, we point out possible research directions on information-theoretic approaches to differential privacy for future work.

2 Preliminaries

This section is reserved for a review of some important preliminaries from the differential privacy literature. We begin with defining the notion of neighborhood of datasets and the sensitivity of differential privacy.

Definition 1. *Two datasets x and $\tilde{x}$ are called neighbors, if the following equality holds*

$$d(x, \tilde{x}) = 1 \tag{1}$$

where $d(.,.)$ denotes the Hamming or l_1 distance between the datasets [11].

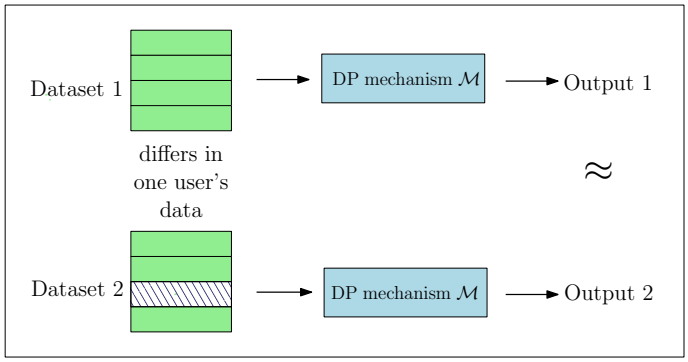

Figure 2: Symmetric neighborhood of differential privacy

Definition 1 considers symmetry among neighbors in terms of the size of the dataset as depicted in Figure 2. This is further relaxed to include the datasets, where neighborhood is due to addition or removal of a record as shown in Figure 1. In both cases, neighbors differ in a single row.

Definition 2. *Global sensitivity, denoted by s, of a function (or a query) $q : D \to \mathbb{R}^k$ is the smallest possible upper bound on the distance between the images of q when applied to two neighboring datasets x and $\tilde{x}$. This means that the l_1 distance is bounded as follows $\|q(x) - q(\tilde{x})\|_1 \leq s$ [28].*

Basically, sensitivity of a differentially private mechanism of Definition 2 is the tightest upper bound on the images of a query (a mapping function) for neighbors. It is a function of the type of the query having an opposite relationship with the privacy, since higher sensitivity of the query refers to a stronger requirement for privacy guarantee, consequently more noise is needed to achieve that guarantee. The original definition of differential privacy makes use of this notion of neighborhood between datasets. An informal definition is depicted in Figure 2. Accordingly, a mechanism $\mathcal{M}$ is said to be differentially private if for any two neighboring datasets, corresponding

outputs of the mechanism, Outputs 1 and 2, are indistinguishable. In other words, the output of a differentially private mechanism is expected to behave in the same way whether or not one contributes the dataset with their data. The following formal definition of differential privacy introduced and studied by Dwork *et al.* in various publications [6, 9, 11] clarifies the mathematical meaning of indistinguishability of the outputs corresponding to neighboring datasets.

Definition 3. *$(\epsilon, \delta)-$ differential privacy: A randomized algorithm $\mathcal{M}$ is $(\epsilon, \delta)-$ differentially private if $\forall S \subseteq Range(\mathcal{M})$ and $\forall x, \tilde{x}$ that are neighbors within the domain of $\mathcal{M}$, the following inequality holds.*

$$\Pr\left[\mathcal{M}(x) \in S\right] \leq \Pr\left[\mathcal{M}(\tilde{x}) \in S\right] \mathrm{e}^{\epsilon} + \delta \tag{2}$$

For two different privacy measures ϵ_1-DP and ϵ_2-DP where $\epsilon_1, \epsilon_2 > 0$, $\epsilon_1 - \mathrm{DP} \succeq \epsilon_2 - \mathrm{DP}$ denotes that ϵ_1- DP is a stronger privacy metric than ϵ_2-DP. Analogous to Definition 3, there are two other cases of differential privacy where either of the privacy parameters, ϵ or δ, equals to zero. The ordering of these three cases from the strongest to the weakest privacy metric is as follows

$$\epsilon - \mathrm{DP} \succeq (\epsilon, \delta) - \mathrm{DP} \succeq \delta - \mathrm{DP}. \tag{3}$$

Dwork's original definition of differential privacy in Definition 3 emanates from a notion of statistical indistinguishability of two different probability distributions given by the next definition.

Definition 4 (Statistical Closeness)**.** *Two probability distributions P_1 and P_2 are said to be $(\epsilon, \delta)-$ close denoted by $P_1 \overset{(\epsilon,\delta)}{\approx} P_2$ over the measurable space $(\Omega, \mathcal{F})$ iff the following inequalities hold.*

$$P_1(A) \leq \mathrm{e}^{\epsilon} P_2(A) + \delta, \quad \forall A \in \mathcal{F} \tag{4}$$

$$P_2(A) \leq \mathrm{e}^{\epsilon} P_1(A) + \delta, \quad \forall A \in \mathcal{F} \tag{5}$$

Some important properties of statistical closeness are reminded here which will be used in Section 3 to prove equality between mutual information functional and differential privacy.

1. Property 1: Statistical closeness have the following relation with Kullback-Leibler divergence.

$$P_1 \overset{(\epsilon,0)}{\approx} P_2 \Longrightarrow \begin{array}{l} D(P_1||P_2) \leq \min\{\epsilon, \epsilon^2\} \\ D(P_2||P_1) \leq \min\{\epsilon, \epsilon^2\} \end{array} \tag{6}$$

   Note that, the right hand sides of the inequalities are given in nats.

2. Property 2: Due to Pinsker's inequality, we also have

$$D(P_1||P_2) \leq \epsilon \text{ nats} \Longrightarrow P_1 \overset{(0,\sqrt{\epsilon/2})}{\approx} P_2. \tag{7}$$

3. Property 3: For any $\epsilon' < \epsilon$ and $\delta' = 1 - \frac{(\mathrm{e}^{\epsilon'}+1)(1-\delta)}{\mathrm{e}^{\epsilon}+1}$, we have the following relation.

$$P_1 \overset{(\epsilon,\delta)}{\approx} P_2 \Longrightarrow P_1 \overset{(\epsilon',\delta')}{\approx} P_2 \tag{8}$$

2.1 How to obtain $\epsilon-$ and $(\epsilon, \delta)-$ differential privacy?

A differentially private mechanism is named after the probability distribution of the perturbation applied onto the query output, in the global setting. In the following, we remind the reader of the Laplace distribution and introduce Laplace and Gaussian mechanisms. The Laplace distribution, also known as the double exponential distribution, with location parameter μ and scale parameter b is defined by

$$Lap(x; \mu, b) = \frac{1}{2b} \mathrm{e}^{-\frac{|x-\mu|}{b}} \tag{9}$$

where its mean equals its location parameter μ and its variance is $2b^2$.

Definition 5. *Laplace mechanism [28] for a function (or a query) $q : D \to \mathbb{R}^k$ is defined by*

$$\mathcal{M}(x, q(.), \epsilon) = q(x) + (Z_1, \cdots, Z_k) \tag{10}$$

where $Z_i \sim Lap(b = s/\epsilon)$, $i = 1, \cdots, k$ denote i.i.d. Laplace random variables.

Definition 6. *Gaussian mechanism [28] is defined for a function (or a query) $q : D \to \mathbb{R}^k$ as follows*

$$\mathcal{M}(x, q(.), \epsilon, \delta) = q(x) + (Z_1, \cdots, Z_k) \tag{11}$$

where $Z_i \sim \mathcal{N}(0, \sigma^2)$, $i = 1, \cdots, k$ denote i.i.d. Gaussian random variables with the variance $\sigma^2 = \frac{2s^2 \log(1.25/\delta)}{\epsilon^2}$.

Theorem 1. *[11] For any $\epsilon, \delta \in (0, 1)$, the Gaussian mechanism satisfies (ε, δ)-differential privacy.*

Remark. *As an alternative to Laplacian perturbation applied on the query output which results in $(\epsilon, 0)-$ differential privacy, Gaussian noise provides a more relaxed privacy guarantee, that is $(\epsilon, \delta)-$ differential privacy. However, in some cases, application of Gaussian noise becomes more useful. Vector valued Laplace mechanisms require the use of l_1- sensitivity whereas the vector-valued Gaussian mechanism allows l_1 or l_2 sensitivity, where l_2 sensitivity is defined as $\max_{x,\tilde{x}} \|q(x) - q(\tilde{x})\|_2 \leq s$, for neighboring x and $\tilde{x}$. Dependent on the query function, when the l_2 sensitivity is significantly lower than l_1 sensitivity, Gaussian mechanism requires much less noise.*

Remark (The optimal $\epsilon-$ differentially private mechanism)**.** *A natural question that comes to mind is if we can do better than the Laplace mechanism. The work in [29] improves the Laplace mechanism of [28] by characterizing the fundamental trade-off between the differentially private mechanism's privacy and utility to define an optimal $\epsilon-$ mechanism. Accordingly, [29, Theorem 1] shows that such a mechanism is obtained by applying a staircase-shaped probability distribution as the perturbation on real and integer-valued query functions in the low-privacy regime (i.e. when ϵ is large). Laplace mechanism outperforms the optimal $(\epsilon, 0)-$ mechanism in the high privacy regime.*

3 Shannon Information and Relative Entropy as a Privacy Constraint

This first main part of the tutorial is dedicated for presentation of information-theoretic quantities adapted to be used as privacy constraint in systems that deploy $(\epsilon, \delta)-$ differential privacy.

Definition 7 ($\epsilon-$Mutual-Information differential privacy (MI-DP) [13])**.** *For a dataset $X^n = (X_1, \cdots, X_n)$ with the corresponding ML output Y according to the randomized mechanism represented by $\mathcal{M} = P_{Y|X^n}$, mutual information differential privacy (MI-DP) is defined as*

$$\sup_{i, P_{X^n}} I(X_i; Y | X^{-i}) \leq \epsilon \text{ nats} \tag{12}$$

where $X^{-i} = \{X_1, \cdots, X_{i-1}, X_{i+1}, \cdots, X_n\}$ denotes the dataset entries excluding X_i.

$\epsilon-$MI-DP definition of Cuff *et al.* in [13] combines the Shannon information with the notion of *identifiability* which is defined using the Bayesian approach on indistinguishability of the neighboring datasets. Accordingly, a mechanism $\mathcal{M}$ satisfies $\epsilon-$**identifiability** for some positive and real ϵ if the following inequality holds for any neighboring entries $x, \tilde{x} \in \mathcal{D}^n$ and any output $y \in \mathcal{D}^n$.

$$P_{X|Y}(x|y) \leq \mathrm{e}^{\epsilon} P_{X|Y}(\tilde{x}|y) \tag{13}$$

Both $\epsilon-$MI-DP and $\epsilon-$identifiability are subject to the implicit strong adversary assumption [13] (also called as the *informed adversary* in [28]) where the adversary has the knowledge of all but a single entry in a dataset and aims to discover the last one. The condition in (13) suggests that for small values of ϵ, neighboring datasets are indistinguishable based on the posterior probabilities of the output. This is what makes it hard to associate the representation of the data and the data owner, which translates to re-identification. Another line of work in [14] defines the mutual information-based differential privacy as a lossy source coding problem without the maximization taken over all possible dataset distributions. Definition 7 differs from the information theoretic definitions of original differential privacy by incorporating that no assumptions are made on prior dataset distributions. Maximization over all possible input distributions in (12) assures that the differential privacy is a property of the mechanism resembling the well-known formula of the Shannon capacity.

Next, we remind the reader of the so-called *Kullback-Leibler differential privacy.*

Definition 8 ($\epsilon-$Kullback-Leibler (KL) differential privacy [13])**.** *A randomized mechanism $P_{Y|X}$ guarantees $\epsilon-$ KL-differential privacy, if the following inequality holds for all its neighboring datasets x and $\tilde{x}$,*

$$D(P_{Y|X=x} || P_{Y|X=\tilde{x}}) \leq \mathrm{e}^{\epsilon}. \tag{14}$$

3.1 Main Result

Using information-theoretic quantities to study privacy may not be a brand new approach, nonetheless, the following result draws the strongest link between the two areas. Ordering and equivalence of $\epsilon-$MI-DP and differential privacy is given by Theorem 2.

Theorem 2 ([13]). *The following chain of inequalities hold*

$$\epsilon - DP \succeq \epsilon - MI\text{-}DP \succeq (\epsilon, \delta) - DP \tag{15}$$

Conditioned on the cardinality of the input $\mathcal{X}_i$ or the output $\mathcal{Y}$ of the differentially private mechanisms, an equivalence is achieved between $\epsilon-$MI-DP and $(\epsilon, \delta)-$ differential privacy. Then, we have

$$\epsilon - MI\text{-}DP = (\epsilon, \delta) - DP \tag{16}$$

The case $(\epsilon, \delta) - DP \succeq \epsilon - MI\text{-}DP$ depends on the cardinality bound $\min\left\{|\mathcal{Y}|, \max_i |\mathcal{X}_i|\right\}$.

The sketch of the proof of Theorem 2 [13] As is well-known, (un/conditional) mutual information can be represented as a function of relative entropy. The proof of Theorem 2 starts off by proving an even more powerful chain of in/equalities among all three variations ϵ, (ϵ, δ) and $\delta-$ differential privacy, mutual information differential privacy and the Kullback-Leibler differential privacy. The chain of inequalities in (15) is expanded out as follows.

$$\epsilon - \text{DP} \overset{(a)}{\succeq} \text{KL} - \text{DP} \overset{(b)}{\succeq} \epsilon - \text{MI} - \text{DP} \overset{(c)}{\succeq} \delta - \text{DP} \overset{(d)}{=} (\epsilon, \delta) - \text{DP} \tag{17}$$

(17) shows that an $\epsilon-$DP mechanism also guarantees $\epsilon-$MI-DP. Relations (a) and (b) in (17) are results of Property 1 of statistical closeness given by Definition 4. Ordering in (b) is achieved as follows

$$D(P_{Y|X^n=x^n} || P_{Y|X^{-i}=x^{-i}}) = D\left(P_{Y|X^n=x^n} || \mathbb{E}\left[P_{Y|X_i=\tilde{X}, X^{-i}=x^{-i}}\right]\right) \tag{18}$$

$$\leq \mathbb{E}\left[D(P_{Y|X^n=x^n} || P_{Y|X^{-i}=\tilde{X}, X^{-i}=x^{-i}})\right] \tag{19}$$

$$\leq \epsilon \text{ nats} \tag{20}$$

for $\tilde{X} \sim P_{X_i|X^{-i}=x^{-i}}$ and x^{-i} denotes an instance of X^{-i}. Thus, in (18) we use $P_{Y|X^{-i}=x^{-i}} = \mathbb{E}\left[P_{Y|X_i=\tilde{X}, X^{-i}=x^{-i}}\right]$. The steps in (19) and (20), respectively follow due to Jensen's inequality and the definition of mutual information based on relative entropy, that is

$$I(X_i; Y|X^{-i}) = \mathbb{E}\left[D(P_{Y|X^n=\bar{X}^n} || P_{Y|X^{-i}=\bar{X}^{-i}})\right] \tag{21}$$

where $\bar{X}^n \sim P_{X^n}$. Ordering (c) that states $\epsilon - \text{MI} - \text{DP} \succeq \delta - \text{DP}$ is a consequence of Lemma 3.

Lemma 3 ([13]). *The following statement is satisfied with respect to the relation between $\epsilon-$MI-DP and $(\delta)-$ DP.*

$$\epsilon - \text{MI} - \text{DP} \Longrightarrow (0, \sqrt{2\epsilon}) - \text{DP} \tag{22}$$

(22) is tightened as $\epsilon - \text{MI} - \text{DP} \Longrightarrow (0, \delta') - \text{DP}$ for $\epsilon \in [0, \ln 2]$ for $\delta' = 1 - 2h^{-1}(\ln 2 - \epsilon)$ and h^{-1} denotes the inverse of the binary entropy function.

Lastly, ordering (d) in (17) is due to Property 3 given by Definition 4. The reader is referred to [13, Section 3.3.] for the full proof.

Remark. *The major strength of $\epsilon-$MI-DP over other alternative mutual information based definitions of differential privacy lies in* ***the maximization taken over all possible input distributions to capture the fact that differential privacy does not require a particular distribution of the input.*** *Moreover, from a stochastic perspective, conditional mutual information reflects the strong adversary assumption of differential privacy and establishes another major strength of $\epsilon-$MI-DP that is based on Dwork's standard definition of differential privacy which originally stems from this assumption. Conditioning on the remaining entries of the dataset in $\epsilon-$MI-DP demonstrates that the adversary has the knowledge of the entire dataset except for one entry, which was transmitted implicitly by using the notion of neighboring datasets in the original stochastic definition of differential privacy. From a practical point of view, another major strength of Definition 7 lies in the ability to transfer information-theoretic rules and properties defined for Shannon information and related measures onto differential privacy.*

Next part provides some of the well-known information-theoretic rules that also apply to differential privacy as a consequence of MI-DP and the ordering in (17).

3.2 Composability of $\epsilon-$MI-DP via information-theoretic rules

This part is dedicated for some of the well-known properties of mutual information which are now directly applicable on $\epsilon-$MI-DP.

1. Bounding the conditional mutual information: If X is independent of Z, then the following inequality holds.

$$I(X;Y|Z) \geq I(X;Y) \tag{23}$$

2. Consequence of data processing inequality: If $X \to Y \to Z$ form a Markov chain in that order that is X and Z are conditionally independent given Y, then the following inequality holds.

$$I(X;Y|Z) \leq I(X;Y) \tag{24}$$

3. Chain rule:

$$I(X;Y,Z) = I(X;Z) + I(X;Y|Z) \tag{25}$$

4. Independence: If the differentially private mechanism $\mathcal{M} = P_{Y|X^n}$ satisfies $\epsilon-$MI-DP where $\{X_i\}_{i=1}^n$ are mutually independent, then the following chain of inequalities hold.

$$\sup_{i,P_{X^n}} I(X_i;Y) \leq \sup_{i,P_{X^n}} I(X_i;Y|X^{-i}) \leq \epsilon \tag{26}$$

Some of the fundamental rules of mutual information enlisted above are transferred onto differential privacy as a result of Theorem 2. Several important properties of differential privacy are straightforward to prove in this mutual information based approach. Next, we prove the composition theorem of differential privacy with the aid of these properties. Originally, composability -an important property of $(\epsilon, 0)-$DP- states that a number of queries under differential privacy also collectively satisfies differential privacy where the privacy budget of the collection is scaled proportionally to the number of queries [30,31]. Corollary 3.1 is a reflection of the composition theorem for $(\epsilon, 0)-$ differential privacy onto $\epsilon-$MI-DP, which shows that the composability can be defined and proven using information-theoretic quantities and their corresponding properties.

Corollary 3.1 (Composition of $\epsilon-$MI-DP [13])**.** *For randomized mechanisms $\mathcal{M}_j = P_{Y_j|X^n}$ that individually satisfy $\epsilon-$MI-DP with k conditionally independent outputs $\{Y_1, \cdots, Y_k\}$ given the input $\{X_1, \cdots, X_n\}$, the collection of k mechanisms $\mathcal{M}_k = P_{Y_k|X^n}$ also satisfies $\epsilon-$MI-DP with the privacy parameter $\sum_j^k \epsilon_j$.*

Proof. For any P_{X^n} and i, the collection of $P_{Y_k|X^n}$ satisfies $\epsilon-$MI-DP which is bounded as follows:

$$I(X_i;Y|X^{-i}) = \sum_{l=1}^{m} I(X_i;Y_l|X^{-i}, Y^{l-1}) \tag{27}$$

$$\leq \sum_{l=1}^{m} I(X_i;Y_l|X^{-i}) \tag{28}$$

(27) follows due to the chain rule given by Property 3 in Section 3.2. Step in (28) uses a property of the data-processing inequality (Property 2 in Section 3.2) due to the conditional independence between X_i and Y^{l-1} given Y_l. Finally, (29) substitutes Definition 7 as given below.

$$I(X_i;Y|X^{-i}) \leq \sum_{l=1}^{m} \epsilon_j \text{ nats} \tag{29}$$

This result completes the first main part of the tutorial.

4 Information-Theoretic Bounds on Differential Privacy

In this section, we review four selective publications [21,32–34] that present upper bounds on the performance of differentially private mechanisms using different metrics. We begin with the two-party differential privacy in the distributed setting in the upcoming part.

4.1 Bounding the Information Cost

Contrarily to the common client-server setting where the server answers queries of clients based on its access policy, in the two-party distributed setting parties execute their analysis on joint data where the aim is to provide a two-sided privacy guarantee for each party's data. In such a setting, each side sees the protocol/mechanism as a differentially private version of the other side's input data. Information cost of a two-user differential privacy model in such a setting refers to the amount of information gathered from each party's inputs using the exchanged messages. In order to prove the usefullness and practicality of differential privacy, McGregor *et al.* characterizes in [21] a fundamental connection between the information cost and differential privacy. Accordingly, the authors presents an upper bound on the information cost of such a mechanism by defining the cost as the mutual information between the inputs and the random transcript of the mechanism denoted $\Pi(.,.)$ which simply is the sequences of exchanged messages between the two parties.

Definition 9 (Information Cost)**.** *For two inputs X and Y of a two-party mechanism $\mathcal{M}$ with probability distribution P, the information cost of the mechanism is defined as*

$$Icost_P(\mathcal{M}) = I(X, Y; \Pi(X, Y)) \tag{30}$$

For a finite alphabet Σ, the two-party $\epsilon-$ differential privacy mechanism $\mathcal{M}(x, y)$ with $x, y \in \Sigma^n$ and every distribution P defined on $\Sigma^n \times \Sigma^n$, the information cost of this mechanism satisfies the upper bound

$$Icost_P(\mathcal{M}) \leq 3\epsilon n. \tag{31}$$

For the special case of $\Sigma = \{0, 1\}$ and P is the uniform distribution, the bound in (31) is improved to $1.5\epsilon^2 n$ [21, Proposition 4.3].

Derivation of the upper bounds For the two-party random input denoted by $T = (X_1, \cdots, X_n, Y_1, \cdots, Y_n)$ and independent sample T' from the uniform distribution P, we have

$$\begin{aligned} I(\Pi(T); T) &= H(\Pi) - H(\Pi|T) \\ &= \mathbb{E}_{(t,\pi)\leftarrow(T,\Pi(T))} \log \frac{\Pr[\Pi[T] = \pi | T = t]}{\Pr[\Pi[T] = \pi]} && (32) \\ &\leq 2(\log_2 \mathrm{e})\epsilon n && (33) \end{aligned}$$

(33) is equivalent to the right hand side of (31) and obtained using the following interval for any t and t'.

$$\mathrm{e}^{(-2\epsilon n)} \leq \frac{\Pr[\Pi(t) = \pi]}{\Pr[\Pi(t') = \pi]} \leq \mathrm{e}^{(2\epsilon n)} \tag{34}$$

The improvement is achieved by setting $\Sigma = \{0, 1\}$ for a uniform distribution P as follows.

$$\begin{aligned} I(T; \Pi(T)) &= \sum_{i\in[2n]} I(T_i; \Pi(T)|T_1 \cdots T_{i-1}) && (35) \\ &= \sum_{i\in[2n]} H(T_i|T_1 \cdots T_{i-1}) - H(T_i|\Pi(T)T_1 \cdots T_{i-1}) && (36) \\ &\leq \sum_{i\in[2n]} (1 - H(\mathrm{e}^{\epsilon}/2)) && (37) \\ &\leq \sum_{i\in[2n]} \frac{\epsilon^2}{2 \ln 2} && (38) \end{aligned}$$

The first term in (36) equals 1 since each T_i is independent and uniform in P. Due to the differential privacy property and the Bayes rule, we have $\forall t_1, \cdots, t_{i-1}, \pi$ the ratio confined in the interval $(\mathrm{e}^{-\epsilon}, \mathrm{e}^{\epsilon})$ as given by

$$\mathrm{e}^{-\epsilon} \leq \frac{\Pr[T_i = 0|T_1, \cdots, T_{i-1} = t_1, \cdots, t_{i-1}, \Pi[T] = \pi]}{\Pr[T_i = 1|T_1, \cdots, T_{i-1} = t_1, \cdots, t_{i-1}, \Pi[T] = \pi]} \leq \mathrm{e}^{\epsilon} \tag{39}$$

Accordingly, the second term in (36) is bounded by the entropy in (37). Finally, in (38), the base of the logarithm is changed and summed over $2n$ terms to get $\log_2(\mathrm{e})\epsilon^2 n$. [35] presents an adaptation of the upper bound in (31) to the mutual information between the distribution over the inputs of an $\epsilon-$ differentially private mechanism and the mechanism's output by replacing the second party's input with a constant to obtain the same behavior of $3\epsilon n$. Accordingly, for a query $q : (\mathbb{Z}^+)^d \to \mathbb{R}^k$, an $\epsilon-$ differentially private mechanism $\mathcal{M} : (\mathbb{Z}^+)^d \to P\mathbb{R}^k$ and a dataset size of n, the mutual information $I(X; \mathcal{M}(X))$ is upper bounded by $3\epsilon n$. Bounding the size of the dataset by n, allows the input distribution to be narrowed down to $X \in [n]^d$ for $[n] = \{0, 1, \cdots, n\}$. This results in the direct application of the upper bound (31) by McGregor *et al.* when the second party's input is set to be a constant.

Remark. *(31) bounds the information cost as a function of the privacy budget of a differentially privacy mechanism and combined with [36], the result signifies that any mechanism that satisfies differential privacy can be compressed. Additionally, well-known bounds for the information cost in various settings can be employed to characterize the gap between the optimal and computational differential privacy mechanisms.*

4.2 Upper bound on maximal leakage

[32] is one of the first examples of the line of work that modeled the problem of defining the optimal mapping of the input data to a privatized output in order to determine the privacy-utility trade-off by using rate-distortion theory. Additionally, the authors compare differential privacy with the maximum information leakage to prove that differential privacy does not grant privacy with regard to average and maximal leakage. Their model is designed as a noiseless communication channel between two parties to transmit a number of measurements denoted $Y \in \mathcal{Y}$ to the receiving end, as well as a set of variables $X \in \mathcal{X}$ which is required to remain private to the sender. X and Y follow the joint distribution $(Y, X) \sim p_{Y,X}(y, x),\ (y, x) \in \mathcal{Y} \times \mathcal{X}$.

$\epsilon-$ *information privacy* is defined as follows in the sense of a differentially private mechanism as a stronger alternative to the Dwork's original definition. Accordingly, $\epsilon-$information privacy captures the fundamental aim of privacy of resisting to notable change in the conditional prior and posterior probabilities of the features given the output.

Definition 10 ([37]). *A privacy preserving mapping defined by the transition probability $p_{Y|\mathbf{X}}(.|.)$ for a set of features $\mathbf{X} = (X_1, \cdots, X_n)$ where $X_i \in \mathcal{X},\ y \in \mathcal{Y}$ provides $\epsilon-$ differential privacy*

$$\mathrm{e}^{-\epsilon} \leq \frac{p_{\mathbf{X}|Y}(\mathbf{x}|y)}{p_{\mathbf{X}}(\mathbf{x})} \leq \mathrm{e}^{\epsilon} \tag{40}$$

for all $y \in \mathcal{Y} : p_Y(y) > 0$ if $\forall x \subseteq \mathcal{X}^n$.

Definition 10 is used for bounding the *maximal (information) leakage* defined by

$$\max_{y \in \mathcal{Y}} H(X) - H(X|Y = y). \tag{41}$$

Maximal leakage refers to the maximum cost gain achieved by the adversary using a single output. The main result of [32] connecting $\epsilon-$ information privacy to differential privacy is given by the next theorem.

Theorem 4 (Upper bound on maximal leakage of differential privacy [32]). *If a privacy-preserving mapping $p_{Y|\mathbf{X}}(.|.)$ is $\epsilon-$ information private for some supp$(p_Y) = \mathcal{Y}$ then it provides at least $2\epsilon-$ differential privacy and the maximal leakage is at most $\frac{\epsilon}{\ln 2}$.*

Proof. For neighbors $\mathbf{x}_1$ and $\mathbf{x}_2$, we have for $p_{Y|\mathbf{X}}(.|.)$ and a subset $B \subseteq \mathcal{Y}$

$$\frac{\Pr[Y \in B|\mathbf{X} = \mathbf{x}_1]}{\Pr[Y \in B|\mathbf{X} = \mathbf{x}_2]} = \frac{\Pr[\mathbf{X} = \mathbf{x}_1|Y \in B]\Pr[\mathbf{X} = \mathbf{x}_2]}{\Pr[\mathbf{X} = \mathbf{x}_2|Y \in B]\Pr[\mathbf{X} = \mathbf{x}_1]} \tag{42}$$

$$\leq \mathrm{e}^{2\epsilon} \tag{43}$$

Bounding step in (43) is a result of Definition 3. The maximum amount of information that is leaked from $\epsilon-$ information private mapping (41) is bounded as given below.

$$H(X) - H(X|Y = y) = \sum_{\mathbf{x} \in \mathcal{X}^n} p_{\mathbf{X}|Y}(\mathbf{x}|y) p_Y(y) \log \left(\frac{p_{\mathbf{X}|Y}(\mathbf{x}|y)}{p_{\mathbf{X}}(\mathbf{x})} \right) \tag{44}$$

$$\overset{(i)}{\leq} \sum_{\mathbf{x} \in \mathcal{X}^n, y \in \mathcal{Y}} p_{\mathbf{X}|Y}(\mathbf{x}|y) p_Y(y) \log \mathrm{e}^{\epsilon} \tag{45}$$

$$\overset{(ii)}{=} \frac{\ln \mathrm{e}^{\epsilon}}{\ln 2} \tag{46}$$

Step (i) results from applying the upper bound of Definition 10 and from changing the range of the sum. In step (ii), the base of the logarithmic function is changed and the summation equals to 1, thus we get $\epsilon / \ln 2$.

4.3 Upper bound on maximal leakage based on min-entropy

This part presents the review of an upper bound on the maximal leakage of $\epsilon-$ differential privacy by [33]. The distinction of the work stems from using *min-entropy* rather than Shannon entropy. The ultimate goal of [33] is to compare and formally characterize connections between differential privacy and information-theoretic leakage. The main contribution is establishing such a connection by upper bounding the information leakage in terms of differential privacy as a function of the privacy budget.

[33] justifies the use of min-entropy by its association to strong security guarantees. For X and Y, respectively denoting the input and output to a probabilistic program and the conditional distribution, $P_{Y|X}$ is characterized by the program's semantics and composes an information-theoretic channel between X and Y. In this setting, the adversary aims to infer the value of X upon reception of the output Y. The unconditional min-entropy $H_\infty(X)$ of X is defined by

$$H_\infty(X) = -\log \max_x P_X(x), \tag{47}$$

whereas the conditional min-entropy $H_\infty(Y|X)$ of $P_{Y|X}$ yields

$$H_\infty(Y|X) = -\log \sum_y P_Y(y) \max_x P_{X|Y}(x,y). \tag{48}$$

The min-entropy-based leakage denoted by L is the difference between $H_\infty(X)$ and $H_\infty(Y|X)$ depending on both the channel $P_{Y|X}$ and the input distribution P_X. Min-entropy based maximal leakage $ML(P_{Y|X})$ is given by

$$ML(P_{Y|X}) = \max_{P_X} (H_\infty(X) - H_\infty(Y|X)). \tag{49}$$

For channels of a single bit of range, that is when $Range(X) = Range(Y) = \{0,1\}$, [33, Theorem 3] states that for an $\epsilon-$ differentially private channel $P_{Y|X}$, the maximal leakage is upper bounded by

$$ML(P_{Y|X}) \leq \log \frac{2\mathrm{e}^\epsilon}{1+\mathrm{e}^\epsilon} \tag{50}$$

The bound in (50) is proven to apply to channels of arbitrary finite range in [33, Corollary 1]. Accordingly, the channel $P_{Y|X}$ is summarized in Table 1 for $\sum_i^n p_i = \sum_i^n q_i = 1$.

Table 1: The channel $P_{Y|X}$ with $X = \{0,1\}$ and $Y = \{y_1, y_2, \cdots, y_n\}$.

$P_{Y\|X}$	$Y = y_1$	$\cdots$	$Y = y_n$
$X = 0$	p_1	$\cdots$	p_n
$X = 1$	q_1	$\cdots$	q_n

For an $\epsilon-$ differentially private channel $P_{\bar{Y}|X}$, where the output $\bar{Y}$ is defined over the range $\{0,1\}$, the leakage of $P_{Y|X}$ and that of $P_{\bar{Y}|X}$ coincide. Similarly, for the channel $P_{\bar{Y}|X}$ we have the following matrix of probabilities for $I = \{i|p_i \leq q_i\}$. In Table 2, $\bar{p}$ and $\bar{q}$ respectively denote the sums over I as $\sum_{i\notin I} p_i$ and $\sum_{i\in I} q_i$. Hence their respective complements yield $1-\bar{p} = \sum_{i\in I} p_i$ and $1-\bar{q} = \sum_{i\notin I} q_i$. Plugging in [33, Theorem 3] with the definition of min-entropy based maximal leakage, the equivalence of $ML(P_{Y|X})$ and $ML(P_{\bar{Y}|X})$ is proven by

$$ML(P_{Y|X}) = \log \sum_y \max_x P_{Y|X}(y,x) \tag{51}$$

$$= \log(\bar{p} + \bar{q}) \tag{52}$$

since (52) is $ML(P_{\bar{Y}|X})$.

Table 2: The channel $P_{\bar{Y}|X}$ with $X, \bar{Y} = \{0,1\}$.

$P_{\bar{Y}\|X}$	$\bar{Y} = 0$	$\bar{Y} = 1$
$X = 0$	$\bar{p}$	$1-\bar{p}$
$X = 1$	$\bar{q}$	$1-\bar{q}$

Additionally, $\epsilon-$differential privacy of the channel $P_{Y|X}$ guarantees that $q_i \leq \mathrm{e}^\epsilon$ for every $i \in I$ and thus, $\bar{q} \leq \mathrm{e}^\epsilon \bar{p}$. Same applies to $p_i \leq \mathrm{e}^\epsilon$ for every $i \notin I$.

4.4 Information-Theoretic Post-processing of Differential Privacy

The post-processing property is one of the important features of differential privacy and ensures that the privacy protection of a differentially private mechanism is not affected by arbitrary computations applied on the mechanism's output [11]. In other words, it is impossible to *undo* the privacy guarantee of differential privacy by post-processing the data. More formally, if the mechanism $\mathcal{M} : \mathbb{N}^{|\mathcal{X}|} \to R$ satisfies $(\epsilon, \delta)-$ differential privacy, for any arbitrary mapping $f : R \to R'$, $f \circ \mathcal{M} : \mathbb{N}^{|\mathcal{X}|} \to R'$ also satisfies $(\epsilon, \delta)-$ differential privacy.

A simpler version of the problem of investigating the connection between differential privacy and min-entropy leakage in [33] is initiated by [34,38] for an individual rather than the entire universe of databases. In [34,38], the authors consider a model where information leakage is used to measure the amount of information that an attacker can learn about the database which also allows to quantify the utility of the query via min-entropy. Applying Bayesian post-processing on the differentially private output of the mechanism, it is shown that the utility function is closely related to conditional min-entropy and to the min-entropy leakage.

5 Differential Privacy as a Source-coding Problem

Several works study the connection between differential privacy and (lossy) source-coding from various aspects [14, 15, 32, 39–41] and some tailored the rate-distortion theory to identify a trade-off between privacy and distortion. [32] is one of the first examples that model differential privacy using a rate-distortion perspective establishing a trade-off between privacy and utility. The authors set the amount of information obtained by the adversary (i.e. the leakage) as the cost gain and minimize it subject to a set of utility constraints, which reflect the role of the distortion function in the original setting of the rate-distortion theory. On the other hand, in [14], the distortion between the input and output of the mechanism is used to determine the number of rows that differ and it is minimized subject to three different privacy metrics, in order to establish how many rows need to be modified to preserve the privacy guarantee. Accordingly, the distortion is defined as the Hamming distance d between the input and output of a dataset as $d : \mathcal{D}^n \times \mathcal{D}^n \to \mathbb{N}$. The contribution of [14] is to demonstrate a connection between identifiability, differential privacy and *the mutual-information privacy* (MIP) that is defined by $I(X;Y)$ for the input X and output Y. The privacy-distortion problem of [14] is defined as follows.

$$\min_{P_{Y|X}} I(X;Y) \tag{53}$$

$$\text{s.t. } \mathbb{E}[d(X,Y)] \leq D, \tag{54}$$

$$\sum_{y \in \mathcal{D}^n} p_{Y|X}(y|x) = 1, \forall x \in \mathcal{D}^n, \tag{55}$$

$$p_{Y|X}(y|x) \geq 0, \forall x, y \in \mathcal{D}^n \tag{56}$$

The main objective of [14] is to investigate and explain the relation between identifiability, differential privacy and MIP in order to compare them. The authors show that there exists a privacy mechanism which minimizes both $I(X;Y)$ and the identifiability. The **privacy-distortion function** denoted as $\epsilon^*(D)$ refers to the smallest differential privacy level for a given maximum allowable distortion D. The mutual information based privacy level is bounded as follows

$$\epsilon^*(D) \leq \epsilon \leq \epsilon^*(D) + 2\epsilon_X \tag{57}$$

where the maximal prior probability difference is

$$\epsilon_X = \max_{x, \tilde{x} \in \mathcal{D}^n : x \sim \tilde{x}} \ln \frac{p_X(x)}{p_X(\tilde{x})} \tag{58}$$

for neighboring datasets x and $\tilde{x}$. This mutual information based mechanism satisfies $\epsilon-$ differential privacy. In light of [13, Theorem 1], which is visited in Section 3, the exact relation and ordering between conditional mutual information and differential privacy are today known.

[40] studies the convergence of the source distribution estimate to the actual distribution based on the output from a locally differentially private mechanism. The fundamental difference in this setting stems from the fact that the differential privacy noise that is applied on each user's data locally, removes the requirement for a notion of neighborhood between datasets. In the model of [40], the source $\{X_i\}$ follows a discrete distribution P and the mechanism $\mathcal{M}$ refers to the application of local differential privacy noise on n i.i.d. source symbols which outputs the privatized observations $\{Y_i\}$ following the distribution Q, that is $P\mathcal{M}$. The goal of the legitimate observer is to estimate the source distribution P using the noisy outputs $\{Y_i\}$ subject to either of f-divergence, mean-squared error (MSE) or total variation as the fidelity criteria. At the same time, an adversary aims to discover some source samples X_i. The authors present upper and lower bounds on their formulation of the trade-off between differential privacy level and fidelity loss based on the aforementioned three loss functions.

5.1 An Adaptation to Adversarial Classification

Introducing adversarial examples to ML systems is a specific type of sophisticated and powerful attack, whereby additional (sometimes specially crafted) or modified inputs are provided to the system with the intent of being misclassified by the model as legitimate. Adversarial classification is one possible defense proposed to correctly detect adversarial examples that aim to fool the classifier which detects outliers. In [18, 42], differential privacy is weaponized by the adversary in order to ensure to remain undetected. In addition to the statistical approach using hypothesis testing to establish a threshold of detection for the adversary as a function of the privacy budget, [42] also introduces an original adaptation of lossy source coding to upper bound the impact of the attack.

In this setting, the adversary not only wants to discover the data but also aims to harm the differentially private mechanism by modifying the released information without being detected. This trade-off between two conflicting goals of adversary is remodeled via the rate-distortion theory balancing the adversary's advantage and the security of the Gaussian differential privacy mechanism. Accordingly, the mutual information between the input and output of a communication channel in the original rate-distortion problem is now replaced by the datasets before and after the alteration applied by the adversary which are considered as neighbors, where the absolute difference between the two corresponds to the impact of the attack. Neighboring input vectors $X^n = \{X_1, \cdots, X_n\}$ and $\tilde{X}^n = \{X_1, \cdots, X_i, \cdots, X_n + X_{adv}\}$ are assumed to be i.i.d following the Gaussian distribution with the parameters $\mathcal{N}(0, \sigma^2_{X_i})$ with the difference of a single record denoted $X_{adv} \sim \mathcal{N}(0, \sigma^2_{adv})$. The query function takes the aggregation of this dataset as $q(\mathbf{X}) = \sum_i^n X_i$ and the DP-mechanism adds Gaussian noise Z on the query output leading to the noisy output in the following form $\mathcal{M}(\mathbf{X}, q(.), \epsilon, \delta) = Y = \sum_i^n X_i + Z$. An adversary adds a single record denoted X_{adv} to this dataset. The modified output of the DP-mechanism becomes $\sum_i^n X_i + X_{adv} + Z$.

Theorem 5. *The privacy-distortion function for a dataset X^n and Gaussian mechanism as defined by Definition (6) is*

$$P(s) = \frac{1}{2} \log \left(f_n \left(1 + \prod_i^n \sigma^2_{X_i} / s^2 \right) \right), \tag{59}$$

for $s \in \left[0, \prod_i^n \sigma^2_{X_i}\right]$ and zero elsewhere. σ_{X_i} denotes the standard deviation of X_i for $i = 1, \cdots, n$, f_n is some constant dependent on the size of the dataset n.

The sketch of the proof proceeds as follows. The mutual information between the datasets before and the attack is derived as follows

$$I(X^n; \tilde{X}^n) = h(\tilde{X}^n) - h(\tilde{X}^n | X^n) \tag{60}$$

$$\geq \frac{1}{2} \sum_{i=1}^n \log \left((2\pi \mathrm{e}) \, \sigma^2_{X_i} \right) - \frac{1}{2} \log \left(2\pi \mathrm{e} s^2 \right) \tag{61}$$

$$= \frac{1}{2} \log \left((2\pi \mathrm{e})^{n-1} \prod_i^n \sigma^2_{X_i} / s^2 \right) \tag{62}$$

Corollary 5.1. *The second order statistics of the additional data inserted into the dataset by the adversary is upper bounded as follows*

$$\sigma^2_{X_{adv}} \leq \frac{1}{(2\pi \mathrm{e})^{n-1}} \left[\frac{s^2}{1 - s^2 / \sigma^2_{X_n}} \right] \tag{63}$$

for $s^2 = \frac{\sigma_z^2 \epsilon^2}{2 \log(1.25/\delta)}$ and $n \geq 2$.

We have the following considering the neighbor that includes X_{adv} has now $(n+1)$ entries over n rows as $\tilde{X}^n = \{X_1, X_2, \cdots, X_n + X_{adv}\}$. Accordingly, the second expansion is derived on X^n as

$$I(X^n; \tilde{X}^n) = h(X^n) - h(X^n | \tilde{X}^n) \tag{64}$$

$$\leq \sum_{i=1}^n \frac{1}{2} \log \left(2\pi \mathrm{e} \right)^n \sigma^2_{X_i} - \frac{1}{2} \log \left((2\pi \mathrm{e})^n \sigma^2_{X_{adv}} \right) \tag{65}$$

$$\leq \frac{1}{2} \log \prod_{i=1}^{n-1} \sigma^2_{X_i} \left(1 + \frac{\sigma^2_{X_n}}{\sigma^2_{X_{adv}}} \right) \tag{66}$$

leading to the upper bound in (63). Due to the adversary's attack, in the first term of (65), we add up the variances of $(n+1)$ X_i's including X_{adv}. Since (62) $\geq$ (66), we obtain the upper bound in Corollary 5.1 For detailed derivation of (62) and (66), the reader is referred to [42].

Remark. *The second expansion of the mutual information between neighboring datasets derived in (66), can be related to the well-known* ***rate-distortion function of the Gaussian source*** *which, originally, provides the minimum possible transmission rate for a given distortion balancing (mostly for the Gaussian case) the squared-error distortion with the source variance. Combining (62) with (66) characterizes the privacy-distortion trade-off of the Gaussian mechanism and bounds the impact of the adversary's modification on the original data in order to avoid detection in some sense calibrating the adversary' attack to the sensitivity of the differentially private mechanism.*

6 What *else* do we want to learn?

As convenient and practical it is, using information-theoretic quantities as privacy constraint is not fully exploited. This final part is reserved for concluding the tutorial by pointing out possible research directions on information-theoretic approaches to differential privacy for the future.

In particular, for classification of adversarial examples in differentially private mechanisms where adversaries may seek for ways to harm the systems via modifying the ML model and misclassifying to model inputs, the source-coding theory could provide new insights in the differential privacy measure itself. A great majority of the existing information theory literature benefits from source coding theory for quantifying the privacy guarantee or for determining the leakage as already mentioned in Section 5. [40] stands out in the way the rate-distortion perspective is translated for differential privacy where various fidelity criteria is set to determine how fast the empirical distribution converges to the actual source distribution. This approach could be extended for detection of adversarial examples attacking differentially private mechanisms beyond the work [18], where the authors presented an application of the Kullback-Leibler differential privacy for detecting misclassification attacks in Laplace mechanisms. The corresponding distributions of relative entropy are considered as the differentially private noise with and without the adversary's advantage. The essential distinction that has to be made as relating differential privacy to mutual information is that the mutual information requires an input distribution. Differential privacy, on the other hand, is a characteristic of the mapping function applied on the input. Consequently, the query mechanism, hence the sensitivity, should play a role in defining the fidelity criterion as translating the adversarial classification into a rate-distortion problem similarly to [42]. Ultimately, this approach inspired by rate-distortion theory could be generalized beyond misclassification attacks for various types of attacks in order to determine and manipulate limits of the impact and detection probability of an attack, and to formally characterize a trade-off between the two. Moreover, by casting differential privacy for adversarial classification into a source coding problem, information-theoretic tools could be used to construct *explicit coding strategies* for privacy preservation in anomaly detection.

Furthermore, information-theoretic quantities could shed light on connections between differential privacy and other trustworthy features of ML algorithms such as fairness and robustness. Various works show pairwise connections of differential privacy with robustness [43–46] and fairness [47]. The knowledge on these relations of differential privacy with these properties are yet to be explored from an information-theoretic perspective.

References

[1] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, pp. 557–570, 2002.

[2] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in *IEEE Symposium on Security and Privacy*. New York, NY, USA: IEEE, May 2008, pp. 111–125.

[3] K. Emam, E. Jonker, L. Arbuckle, and B. Malin, "A systematic review of re-identification attacks on health data," *Plos One PMC*, vol. 6, pp. 1–12, 2011.

[4] H. Zang and J. Bolot, "Anonymization of location data does not work: A large-scale measurement study," in *Proc. Int. Conf. on Mobile Computing and Networking 17*. New York, NY, USA: ACM, Sep. 2011, pp. 145—-156.

[5] A. Chawla, "Pegasus spyware – a privacy killer," Jul 2021. [Online]. Available: SSRN

[6] C. Dwork, "Differential privacy," in *Automata, Languages and Programming*. Berlin, Heidelberg: Springer, 2006, pp. 1–12.

[7] U. Erlingsson, V. Pihur, and A. Korolova, "RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response," in *ACM SIGSAC Conference on Computer and Communications*. New York, NY, USA: ACM, Nov. 2014, pp. 1054–1067.

[8] A. Machanavajjhala, D. Kifer, J. Abowd, J. Gehrke, and L. Vilhuber, "Privacy: Theory meets practice on the map," in *IEEE 24th International Conference on Data Engineering*. New York, NY, USA: IEEE, 2008, pp. 277–286.

[9] C. Dwork, "Differential privacy: A survey of results," in *International Conference on Theory and Applications of Models of Computation TAMC 2008, LNCS 4978*. Berlin, Heidelberg: Springer, 2008, pp. 1–19.

[10] C. Dwork and A. Smith, "Differential privacy for statistics: What we know and what we want to learn," *Journal of Privacy and Confidentiality*, vol. 1, pp. 135–154, 2010.

[11] C. Dwork and A. Roth, "The Algorithmic Foundations of Differential Privacy," *Foundations and Trends in Theoretical Computer Science 2014*, vol. 9, pp. 211–407, 2014.

[12] Z. Lin, M. Hewett, and R. Altman, "Using binning to maintain confidentiality of medical data," in *AMIA 2002 Annual Symposium Proceedings*, Nov. 2002, pp. 454–458.

[13] P. Cuff and L. Yu, "Differential Privacy as a Mutual Information Constraint," in *CCS 2016, Vienna, Austria*. New York, NY, United States: Association for Computing Machinery, Oct. 2016, pp. 43–54.

[14] W. Wang, L. Ying, and J. Zhang, "On the relation between identifiability, differential privacy and mutual information privacy," *IEEE Transactions on Information Theory*, vol. 62, pp. 5018–5029, Sep. 2016.

[15] D. Mir, "Information theoretic foundations of differential privacy," in *International Symposium of Foundations on Practice of Security*. Berlin, Heidelberg: Springer, Oct. 2012, pp. 374–381.

[16] M. Bellare, S. Tessaro, and A. Vardy, "Semantic security for the wiretap channel," in *Advances in Cryptology-CRYPTO*. Berlin, Heidelberg: Springer, 2012, pp. 294–311.

[17] G. Wu, X. Xia, and Y. He, "Achieving dalenius' goal of data privacy with practical assumptions," May 2021. [Online]. Available: https://arxiv.org/abs/1703.07474v5

[18] A. Ünsal and M. Önen, "A Statistical Threshold for Adversarial Classification in Laplace Mechanisms," in *IEEE Information Theory Workshop 2021*. New York, NY, USA: IEEE, Oct. 2021, pp. 1–6.

[19] D. Pankratov, "Communication complexity and information complexity," Ph.D. dissertation, The University of Chicago, Jun. 2015.

[20] Z. Bar Yossef, T. Jayram, R. Kumar, and D. Sivakumar, "An information statistics approach to data stream and communication complexity," *Journal of Computer and System Sciences*, vol. 68, pp. 702–732, Jun. 2004.

[21] A. McGregor, I. Mironov, T. Pitassi, O. Reingold, K. Talwar, and S. Vadhan, "The limits of two-party differential privacy," in *51st Annual Symposium on Foundations of Computer Science (FOCS)*. 1730 Massachusetts Ave., NW Washington, DC, United States: IEEE Computer Society, Oct. 2010, pp. 81–90.

[22] P. Lin, C. Kuhn, T. Strufe, and E. Jorswieck, "Physical layer privacy in broadcast channels," in *2019 IEEE International Workshop on Information Forensics and Security (WIFS)*. Delft, Netherlands: IEEE, Dec. 2019, pp. 1–6.

[23] D. Mir, "Differentially-private learning and information theory," in *International Workshop on Privacy and Anonymity in the Information Society PAIS*. New York, NY, USA: ACM, Mar. 2012, pp. 206–210.

[24] C. Hirche, C. Rouzé, and D. França, "Quantum differential privacy: An information theory perspective," Feb. 2022. [Online]. Available: https://arxiv.org/abs/2202.10717

[25] S. Aaronson and G. N. Rothblum, "Gentle measurement of quantum states and differential privacy," in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, ser. STOC 2019. New York, NY, USA: Association for Computing Machinery, 2019, p. 322–333. [Online]. Available: https://doi.org/10.1145/3313276.3316378

[26] L. Zhou and M. Ying, "Differential privacy in quantum computation," *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*, pp. 249–262, 2017.

[27] M. Senekane, M. Mafu, and B. Taele, "Privacy-preserving quantum machine learning using differential privacy," in *2017 IEEE AFRICON*, ser. 2017 IEEE AFRICON: Science, Technology and Innovation for Africa, AFRICON 2017, D. Cornish, Ed. United States: Institute of Electrical and Electronics Engineers Inc., Nov. 2017, pp. 1432–1435, iEEE AFRICON 2017 ; Conference date: 18-09-2017 Through 20-09-2017.

[28] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating Noise to Sensitivity in Private Data Analysis," in *Theory of Cryptography Conference*. International Association for Cryptologic Research, 2006, pp. 265–284.

[29] Q. Geng and P. Viswanath, "The optimal mechanism in differential privacy," in *IEEE International Symposium on Information Theory*. New York, NY, USA: IEEE, Jul. 2014, pp. 2371–2375.

[30] C. Dwork, G. Rothblum, and S. Vadhan, "Boosting and differential privacy," in *51st Annual Symposium on Foundations of Computer Science (FOCS)*. 1730 Massachusetts Ave., NW Washington, DC, United States: IEEE Computer Society, Oct. 2010, pp. 51–60.

[31] P. Kairouz, S. Oh, and P. Viswanath, "The composition theorem for differential privacy," in *32nd International Conference on Machine Learning*. JMLR, Inc. and Microtome Publishing (United States), 2015, pp. 4037–4049.

[32] F. du Pin Calmon and N. Fawaz, "Privacy against statistical inference," in *Fiftieth Annual Allerton Conference*. New York, NY, USA: IEEE, Oct. 2012, pp. 1401–1408.

[33] G. Barthe and B. Köpf, "Information-theoretic bounds for differentially private mechanisms," in *Computer Security Foundations Symposium*. New York, NY, USA: IEEE, 2011, pp. 191–204.

[34] 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 *Formal Aspects of Security and Trust*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 39–54.

[35] A. De, "Lower bounds in differential privacy," in *Theory of Cryptography Conference*. International Association for Cryptologic Research, Mar. 2012, pp. 321–338.

[36] B. Barak, M. Braverman, X. Chen, and A. Rao, "How to compress interactive communication," in *42nd ACM Symposium on Theory of Computing*. New York, NY, USA: ACM, Jun. 2010, pp. 67–76.

[37] A. Evfimievski, J. Gehrke, and R. Srikant, "Limiting privacy breaches in privacy preserving data mining," in *22nd ACM Symposium on Principles of Database Systems*. New York, NY, USA: ACM, Jun. 2003, pp. 211–222.

[38] M. S. Alvim, K. Chatzikokolakis, P. Degano, and C. Palamidessi, "Differential privacy versus quantitative information flow," *ArXiv*, vol. abs/1012.4250, 2010.

[39] S. Zhou, K. Ligett, and L. Wasserman, "Differential privacy with compression," in *IEEE International Symposium on Information Theory, ISIT*. New York, NY, USA: IEEE, Jun. 2009, pp. 2718–2722.

[40] A. Pastore and M. Gastpar, "Locally differentially private randomized response for discrete distribution learning," *Journal on Machine Learning Research*, vol. 22, pp. 1–56, Jul. 2021.

[41] A. Padakandla, P. Kumar, and W. Szpankowski, "Trade-off between privacy and fidelity vie ehrhart theory," *IEEE Transactions on Information Theory*, vol. 66, pp. 2549–2569, Apr. 2020.

[42] A. Ünsal and M. Önen, "Calibrating the attack to sensitivity in differentially private mechanisms," *Journal of Cybersecurity and Privacy*, vol. 2, no. 4, pp. 830–852, 2022. [Online]. Available: https://www.mdpi.com/2624-800X/2/4/42

[43] M. Du, R. Jia, and D. Song, "Robust anomaly detection and backdoor attack detection via differential privacy," in *International Conference on Learning Representations ICLR 2020*, Sep. 2020.

[44] N. Phan, M. T. Thai, H. Hu, R. Jin, T. Sun, and D. Dou, "Scalable differential privacy with certified robustness in adversarial learning," in *Proceedings of the 37th International Conference on Machine Learning*, ser. ICML'20. JMLR.org, 2020.

[45] R. Pinot, F. Yger, C. Gouy-Pailler, and J. Atif, "A unified view on differential privacy and robustness to adversarial examples," in *Workshop on Machine Learning for CyberSecurity at ECMLPKDD 2019*, Wurzburg, Germany, Sep. 2019. [Online]. Available: https://hal.science/hal-02892170

[46] M. Lecuyer, V. Atlidakis, R. Geambasu, D. Hsu, and S. Jana, "Certified robustness to adversarial examples with differential privacy," in *IEEE Symposium on Security and Privacy, San Francisco CA, USA*, May 2019, pp. 1054–1067.

[47] F. Fioretto, C. Tran, P. Van Hentenryck, and K. Zhu, "Differential privacy and fairness in decisions and learning tasks: A survey," in *Proceedings of the Thirty-First International Joint Conference on Artificial Intelligence, IJCAI-22*, L. D. Raedt, Ed. International Joint Conferences on Artificial Intelligence Organization, 7 2022, pp. 5470–5477, survey Track. [Online]. Available: https://doi.org/10.24963/ijcai.2022/766