Gaussian Differential Privacy

Jinshuo Dong, Aaron Roth, and Weijie J. Su

University of Pennsylvania, Philadelphia, USA

E-mail: jinshuo@sas.upenn.edu, aaroth@cis.upenn.edu, suw@wharton.upenn.edu

[Read before The Royal Statistical Society at an online meeting organized by the Research Section on Wednesday, December 16th, 2020, Professor G. P. Nason in the Chair]

Summary.

In the past decade, differential privacy has seen remarkable success as a rigorous and practical formalization of data privacy. This privacy definition and its divergence based relaxations, however, have several acknowledged weaknesses, either in handling composition of private algorithms or in analyzing important primitives like privacy amplification by subsampling. Inspired by the hypothesis testing formulation of privacy, this paper proposes a new relaxation of differential privacy, which we term "f-differential privacy" (f-DP). This notion of privacy has a number of appealing properties and, in particular, avoids difficulties associated with divergence based relaxations. First, f-DP faithfully preserves the hypothesis testing interpretation of differential privacy, thereby making the privacy guarantees easily interpretable. In addition, f-DP allows for lossless reasoning about composition in an algebraic fashion. Moreover, we provide a powerful technique to import existing results proven for the original differential privacy definition to f-DP and, as an application of this technique, obtain a simple and easy-to-interpret theorem of privacy amplification by subsampling for f-DP.

In addition to the above findings, we introduce a canonical single-parameter family of privacy notions within the f-DP class that is referred to as "Gaussian differential privacy" (GDP), defined based on hypothesis testing of two shifted Gaussian distributions. GDP is the focal privacy definition among the family of f-DP guarantees due to a central limit theorem for differential privacy that we prove. More precisely, the privacy guarantees of *any* hypothesis testing based definition of privacy (including the original differential privacy definition) converges to GDP in the limit under composition. We also prove a Berry–Esseen style version of the central limit theorem, which gives a computationally inexpensive tool for tractably analyzing the exact composition of private algorithms.

Taken together, this collection of attractive properties render f-DP a mathematically coherent, analytically tractable, and versatile framework for private data analysis. Finally, we demonstrate the use of the tools we develop by giving an improved analysis of the privacy guarantees of noisy stochastic gradient descent.

Keywords: Differential privacy; Trade-off function; Composition; Central limit theorem; Primal-dual perspective; Subsampling; Privacy amplification; Blackwell theorem; Private stochastic gradient descent

1. Introduction

Modern statistical analysis and machine learning are overwhelmingly applied to data concerning *people*. Valuable datasets generated from personal devices and online behavior of billions of individuals contain data on location, web search histories, media consumption, physical activity, social networks, and more. This is on top of continuing large-scale analysis of traditionally sensitive data records, including those collected by hospitals, schools, and the Census. This reality requires the development of tools to perform large-scale data analysis in a way that still protects the *privacy* of individuals represented in the data.

Unfortunately, the history of data privacy for many years consisted of ad-hoc attempts at "anonymizing" personal information, followed by high profile de-anonymizations. This includes the release of AOL search logs, de-anonymized by the *New York Times* (Barbaro and Zeller, 2006), the Netflix Challenge dataset, de-anonymized by Narayanan and Shmatikov (2008), the realization that participants in genome-wide association studies could be identified from aggregate statistics such as minor allele frequencies that were publicly released (Homer et al., 2008), and the reconstruction of individual-level census records from aggregate statistical releases (Abowd, 2018).

Thus, we urgently needed a rigorous and principled privacy-preserving framework to prevent breaches of personal information in data analysis. In this context, *differential privacy* has put private data analysis on firm theoretical foundations (Dwork et al., 2006b,a). This definition has become tremendously successful; in addition to an enormous and growing academic literature, it has been adopted as a key privacy technology by Google (Erlingsson et al., 2014), Apple (Apple, 2017), Microsoft (Ding et al., 2017), and the US Census Bureau (Abowd, 2018). The definition of this concept involves privacy parameters $\varepsilon \geq 0$ and $0 \leq \delta \leq 1$.

Definition 1 (Dwork et al. (2006b,a))**.** *A randomized algorithm M that takes as input a dataset consisting of individuals is (ε, δ)-differentially private (DP) if for any pair of datasets S, S' that differ in the record of a single individual, and any event E,*

$$\mathbb{P}\left[M(S) \in E\right] \leqslant \mathrm{e}^{\varepsilon}\mathbb{P}\left[M(S') \in E\right] + \delta. \tag{1}$$

When $\delta = 0$, the guarantee is simply called ε-DP.

In this definition, datasets are *fixed* and the probabilities are taken *only* over the randomness of the mechanism. In particular, the event E can take any measurable set in the range of M. To achieve differential privacy, a mechanism is necessarily randomized. For example, consider the problem of privately releasing the average cholesterol level of individuals in the dataset $S = (x_1, \ldots, x_n)$, where x_i corresponds to the cholesterol level of individual i. A privacy-preserving mechanism may take the form

$$M(S) = \frac{x_1 + \cdots + x_n}{n} + \text{noise}.$$

The level of the noise has to be large enough to mask the *characteristics* of any individual's cholesterol level, while *not* being too large to distort the population average for accuracy purposes. Consequently, the probability distributions of $M(S)$ and $M(S')$ are close to each other for any datasets S, S' that differ in only one individual record.

Differential privacy is most naturally defined through a hypothesis testing problem from the perspective of an attacker who aims to distinguish S from S' based on the output of the mechanism. This statistical viewpoint was first observed by Wasserman and Zhou (2010) and then further developed by Kairouz et al. (2017), which is a direct inspiration for our work. In short, consider the hypothesis testing problem

$$H_0 : \text{the underlying dataset is } S \quad \text{versus} \quad H_1 : \text{the underlying dataset is } S' \tag{2}$$

and call Alice the only individual that is in S but not S'. As such, rejecting the null hypothesis corresponds to the detection of absence of Alice, whereas accepting the null hypothesis means to detect the presence of Alice in the dataset. Using the output of an (ε, δ)-DP mechanism, the power of any test at significance level $0 < \alpha < 1$ has an upper bound of $\mathrm{e}^{\varepsilon}\alpha + \delta$. This bound is only slightly larger than α provided that ε, δ are small and, therefore, *any* test is essentially powerless. Put differently, differential privacy with small privacy parameters protects against any inferences of the presence of Alice, or any other individual, in the dataset.

Despite its apparent success, there are good reasons to want to relax the original definition of differential privacy, which has led to a long line of proposals for such relaxations. The most important shortcoming is that (ε, δ)-DP does not tightly handle composition. Composition concerns how privacy guarantees degrade under repetition of mechanisms applied to the same dataset, rendering the design of differentially private algorithms *modular*. Without compositional properties, it would be near impossible to develop complex differentially private data analysis methods. Although it has been known since the original papers defining differential privacy (Dwork et al., 2006b,a) that the composition of an $(\varepsilon_1, \delta_1)$-DP mechanism and an $(\varepsilon_2, \delta_2)$-DP mechanism yields an $(\varepsilon_1 + \varepsilon_2, \delta_1 + \delta_2)$-DP mechanism, the corresponding upper bound $\mathrm{e}^{\varepsilon_1+\varepsilon_2}\alpha + \delta_1 + \delta_2$ on the power of any test at significance level α no longer tightly characterizes the trade-off between significance level and power for the testing between S and S'. In Dwork et al. (2010), the authors gave an improved composition theorem, but it fails to capture the correct hypothesis testing trade-off. This is for a fundamental reason: (ε, δ)-DP is mis-parameterized in the sense that the guarantees of the composition of $(\varepsilon_i, \delta_i)$-DP mechanisms cannot be characterized by any single pair of parameters (ε, δ). Even worse, given any δ, finding the smallest parameter ε for composition of a sequence of differentially private algorithms is computationally hard (Murtagh and Vadhan, 2016), and so in practice, one must resort to approximations. Given that composition and modularity are first-order desiderata for a useful privacy definition, these are substantial drawbacks and often continue to push practical algorithms with meaningful privacy guarantees out of reach.

In light of this, substantial recent effort has been devoted to developing relaxations of differential privacy for which composition can be handled exactly. This line of work includes several variants of "concentrated differential privacy" (Dwork and Rothblum, 2016; Bun and Steinke, 2016), "Rényi differential privacy" (Mironov, 2017), and "truncated concentrated differential privacy" (Bun et al., 2018a). These definitions are tailored to be able to exactly and easily track the "privacy cost" of compositions of the most basic primitive in differential privacy, which is the perturbation of a real valued statistic with Gaussian noise.

While this direction of privacy relaxation has been quite fruitful, there are still several places one might wish for improvement. First, these notions of differential privacy no longer have hypothesis testing interpretations, but are rather based on studying divergences that satisfy a certain information processing inequality. There are good reasons to prefer definitions based on hypothesis testing. Most immediately, hypothesis testing based definitions provide an easy way to interpret the guarantees of a privacy definition. More fundamentally, a theorem due to Blackwell (see Theorem 2) provides a formal sense in which a tight understanding of the trade-off between type I and type II errors for the hypothesis testing problem of distinguishing between $M(S)$ and $M(S')$ contains only more information than any divergence between the distributions $M(S)$ and $M(S')$ (so long as the divergence satisfies the information processing inequality).

Second, certain simple and fundamental primitives associated with differential privacy—most notably, *privacy amplification by subsampling* (Kasiviswanathan et al., 2011)—either fail to apply to the existing relaxations of differential privacy, or require a substantially complex analysis (Wang et al., 2018). This is especially problematic when analyzing privacy guarantees of stochastic gradient descent—arguably the most popular present-day optimization algorithm—as subsampling is inherent to this algorithm. At best, this difficulty arising from using these relaxations could be overcome by using complex technical machinery. For example, it necessitated Abadi et al. (2016) to develop the numerical *moments accountant* method to sidestep the issue.

1.1. Our Contributions

In this work, we introduce a new relaxation of differential privacy that avoids these issues and has other attractive properties. Rather than giving a "divergence" based relaxation of differential privacy, we start fresh from the hypothesis testing interpretation of differential privacy, and obtain a new privacy definition by allowing the *full* trade-off between type I and type II errors in the simple hypothesis testing problem (2) to be governed by some function f. The functional privacy parameter f is to this new definition as (ε, δ) is to the original definition of differential privacy. Notably, this definition that we term f-differential privacy (f-DP)—which captures (ε, δ)-DP as a special case—is accompanied by a powerful and elegant toolkit for reasoning about composition. Here, we highlight some of our contributions:

An Algebra for Composition. We show that our privacy definition is *closed* and *tight* under composition, which means that the trade-off between type I and type II errors that results from the composition of an f_1-DP mechanism with an f_2-DP mechanism can always be *exactly* described by a certain function f. This function can be expressed via f_1 and f_2 in an algebraic fashion, thereby allowing for losslessly reasoning about composition. In contrast, (ε, δ)-DP or any other privacy definition artificially restricts itself to a small number of parameters. By allowing for a *function* to keep track of the privacy guarantee of the mechanism, our new privacy definition avoids the pitfall of premature summarization (to quote Holmes (2019), "premature summarization is the root of all evil in statistics.") in intermediate steps and, consequently, yields a comprehensive delineation of the overall privacy guarantee. See more details in Section 3.

A Central Limit Phenomenon. We define a single-parameter family of f-DP that

uses the type I and type II error trade-off in distinguishing the standard normal distribution $\mathcal{N}(0,1)$ from $\mathcal{N}(\mu,1)$ for $\mu \geq 0$. This is referred to as Gaussian differential privacy (GDP). By relating to the hypothesis testing interpretation of differential privacy (2), the GDP guarantee can be interpreted as saying that determining whether or not Alice is in the dataset is at least as difficult as telling apart $\mathcal{N}(0,1)$ and $\mathcal{N}(\mu,1)$ based on one draw. Moreover, we show that GDP is a "canonical" privacy guarantee in a fundamental sense: for any privacy definition that retains a hypothesis testing interpretation, we prove that the privacy guarantee of composition with an appropriate scaling converges to GDP in the limit. This central limit theorem type of result is remarkable not only because of its profound theoretical implication, but also for providing a computationally tractable tool for analytically approximating the privacy loss under composition. Figure 1 demonstrates that this tool yields surprisingly accurate approximations to the exact trade-off in testing the hypotheses (2) or substantially improves on the existing privacy guarantee in terms of type I and type II errors. See Section 2.2 and Section 3 for a thorough discussion.

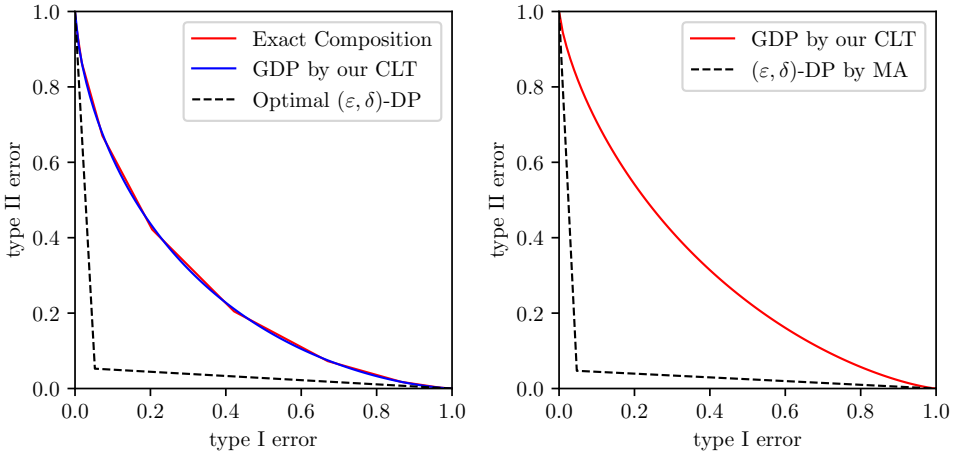

Fig. 1: Left: Our central limit theorem based approximation (in blue) is very close to the composition of just 10 mechanisms (in red). The tightest possible approximation via an (ε,δ)-DP guarantee (in back) is substantially looser. See Figure 5 for parameter setup. Right: Privacy analysis of stochastic gradient descent used to train a convolutional neural network on MNIST (LeCun and Cortes, 2010). The f-DP framework yields a privacy guarantee (in red) for this problem that is significantly better than the optimal (ε,δ)-DP guarantee (in black) that is derived from the moments accountant (MA) method (Abadi et al., 2016). Put simply, our analysis shows that stochastic gradient descent releases less sensitive information than expected in the literature. See Section 5 for more plots and details.

A Primal-Dual Perspective. We show a general duality between f-DP and infinite collections of (ε,δ)-DP guarantees. This duality is useful in two ways. First, it allows one to analyze an algorithm in the framework of f-DP, and then convert back to an (ε,δ)-DP guarantee at the end, if desired. More fundamentally, this duality provides an approach to import techniques developed for (ε,δ)-DP to the framework of f-DP.

As an important application, we use this duality to show how to reason simply about privacy amplification by subsampling for f-DP, by leveraging existing results for (ε, δ)-DP. This is in contrast to divergence based notions of privacy, in which reasoning about amplification by subsampling is difficult.

Taken together, this collection of attractive properties render f-DP a mathematically coherent, computationally efficient, and versatile framework for privacy-preserving data analysis. To demonstrate the practical use of this hypothesis testing based framework, we give a substantially sharper analysis of the privacy guarantees of noisy stochastic gradient descent, improving on previous special-purpose analyses that reasoned about divergences rather than directly about hypothesis testing (Abadi et al., 2016). This application is presented in Section 5.

2. f-Differential Privacy and Its Basic Properties

In Section 2.1, we give a formal definition of f-DP. Section 2.2 introduces Gaussian differential privacy, a special case of f-DP. In Section 2.3, we highlight some appealing properties of this new privacy notation from an information-theoretic perspective. Next, Section 2.4 offers a profound connection between f-DP and (ε, δ)-DP. Finally, we discuss the group privacy properties of f-DP.

Before moving on, we first establish several key pieces of notation from the differential privacy literature.

- **Dataset.** A dataset S is a collection of n records, each corresponding to an individual. Formally, we write the dataset as $S = (x_1, \ldots, x_n)$, and an individual $x_i \in X$ for some abstract space X. Two datasets $S' = (x'_1, \ldots, x'_n)$ and S are said to be *neighbors* if they differ in exactly one record, that is, there exists an index j such that $x_i = x'_i$ for all $i \neq j$ and $x_j \neq x'_j$.
- **Mechanism.** A mechanism M refers to a randomized algorithm that takes as input a dataset S and releases some (randomized) statistics $M(S)$ of the dataset in some abstract space Y. For example, a mechanism can release the average salary of individuals in the dataset plus some random noise.

2.1. Trade-off Functions and f-DP

All variants of differential privacy informally require that it be hard to *distinguish* any pairs of neighboring datasets based on the information released by a private a mechanism M. From an attacker's perspective, it is natural to formalize this notion of "indistinguishability" as a hypothesis testing problem for two neighboring datasets S and S':

$$H_0 : \text{the underlying dataset is } S \quad \text{versus} \quad H_1 : \text{the underlying dataset is } S'.$$

The output of the mechanism M serves as the basis for performing the hypothesis testing problem. Denote by P and Q the probability distributions of the mechanism applied to the two datasets, namely $M(S)$ and $M(S')$, respectively. The fundamental difficulty in distinguishing the two hypotheses is best delineated by the *optimal* trade-off between the achievable type I and type II errors. More precisely, consider a rejection rule $0 \leq \phi \leq 1$

that takes as input the released results of the mechanism, with its type I and type II errors defined as

$$\alpha_\phi = \mathbb{E}_P[\phi], \quad \beta_\phi = 1 - \mathbb{E}_Q[\phi],$$

respectively. The two errors satisfy, for example, the well-known constraint $\alpha_\phi + \beta_\phi \geq 1 - \mathrm{TV}(P, Q)$, where the total variation distance $\mathrm{TV}(P, Q)$ is the supremum of $|P(A) - Q(A)|$ over all measurable sets A. Instead of this rough constraint, we seek to characterize the fine-grained trade-off between the two errors. Explicitly, fixing the type I error at *any* level, we consider the minimal achievable type II error. This motivates the following definition.

Definition 2 (trade-off function)**.** *For any two probability distributions P and Q on the same space, define the trade-off function $T(P, Q) : [0, 1] \to [0, 1]$ as*

$$T(P, Q)(\alpha) = \inf \{\beta_\phi : \alpha_\phi \leqslant \alpha\},$$

where the infimum is taken over all (measurable) rejection rules.

The trade-off function serves as a clear-cut boundary of the achievable and unachievable regions of type I and type II errors, rendering itself the *complete* characterization of the fundamental difficulty in testing between the two hypotheses. The greater this function is, the harder it is to distinguish the two distributions. In particular, the greatest trade-off function is the identity trade-off function $\mathrm{Id}(\alpha) := 1 - \alpha$. Notably, $1 - f$ is the ROC curve for classifying the output as being from the null or alternative hypothesis. For completeness, the minimal β_ϕ can be achieved by the likelihood ratio test—a fundamental result known as the Neyman–Pearson lemma, which is stated in Appendix A for convenience.

A function is called a trade-off function if it is equal to $T(P, Q)$ for some distributions P and Q. Below we give a necessary and sufficient condition for f to be a trade-off function and relegate its proof to Appendix A. This characterization reveals, for example, that $\max\{f, g\}$ is a trade-off function if both f and g are trade-off functions.

Proposition 1. *A function $f : [0, 1] \to [0, 1]$ is a trade-off function if and only if f is convex, continuous, non-increasing, and $f(x) \leqslant 1 - x$ for $x \in [0, 1]$.*

Now, we propose a new generalization of differential privacy built on top of trade-off functions. Below, we write $g \geq f$ for two functions defined on $[0, 1]$ if $g(x) \geq f(x)$ for all $0 \leq x \leq 1$, and we abuse notation by identifying $M(S)$ and $M(S')$ with their corresponding probability distributions. Note that if $T(P, Q) \geq T(\widetilde{P}, \widetilde{Q})$, then in a very strong sense, P and Q are harder to distinguish than $\widetilde{P}$ and $\widetilde{Q}$ at *any* level of type I error.

Definition 3 (f-differential privacy)**.** *Let f be a trade-off function. A mechanism M is said to be f-differentially private if*

$$T\big(M(S), M(S')\big) \geq f$$

for all neighboring datasets S and S'.

A graphical illustration of this definition is shown in Figure 2. Letting P and Q be the distributions such that $f = T(P, Q)$, this privacy definition amounts to saying that a mechanism is f-DP if distinguishing any two neighboring datasets based on the released information is at least as difficult as distinguishing P and Q based on a single draw. In contrast to existing definitions of differential privacy, our new definition is parameterized by a function, as opposed to several real valued parameters (e.g. ε and δ). This functional perspective offers a complete characterization of "privacy", thereby avoiding the pitfall of summarizing statistical information too early. This fact is crucial to the development of a composition theorem for f-DP in Section 3. Although this completeness comes at the cost of increased complexity, as we will see in Section 2.2, a simple family of trade-off functions can often closely capture privacy loss in many scenarios.

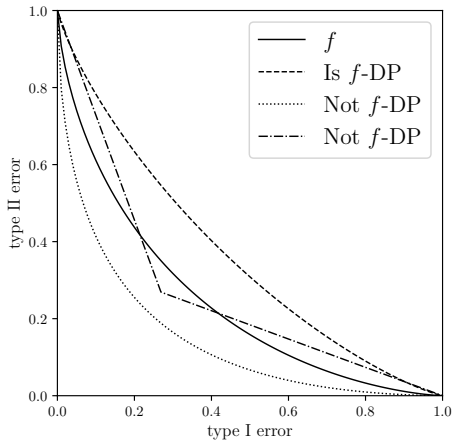

Fig. 2: Three different examples of $T\big(M(S), M(S')\big)$. Only the dashed line corresponds to a trade-off function satisfying f-DP.

Naturally, the definition of f-DP is symmetric in the same sense as the neighboring relationship, which by definition is symmetric. Observe that this privacy notion also requires

$$T\big(M(S'), M(S)\big) \geq f$$

for any neighboring pair S, S'. Therefore, it is desirable to restrict our attention to "symmetric" trade-off functions. Proposition 2 shows that this restriction does not lead to any loss of generality.

Proposition 2. *Let a mechanism M be f-DP. Then, M is f^{S}-DP with $f^{\mathrm{S}} = \max\{f, f^{-1}\}$, where the inverse function is defined as*

$$f^{-1}(\alpha) := \inf\{t \in [0,1] : f(t) \leqslant \alpha\} \tag{3}$$

for $\alpha \in [0, 1]$.

We prove Proposition 2 in Appendix A. Writing $f = T(P, Q)$, we can express the inverse as $f^{-1} = T(Q, P)$, which therefore is also a trade-off function. As a consequence

of this, f^{S} continues to be a trade-off function by making use of Proposition 1 and, moreover, is *symmetric* in the sense that

$$f^{\mathrm{S}} = (f^{\mathrm{S}})^{-1}.$$

Importantly, this symmetrization gives a tighter bound in the privacy definition since $f^{\mathrm{S}} \geqslant f$. In the remainder of the paper, therefore, trade-off functions will always be assumed to be symmetric unless otherwise specified.

We conclude this subsection by showing that f-DP is a generalization of (ε, δ)-DP. This foreshadows a deeper connection between f-DP and (ε, δ)-DP that will be discussed in Section 2.4. Denote

$$f_{\varepsilon,\delta}(\alpha) = \max\left\{0, 1-\delta-\mathrm{e}^{\varepsilon}\alpha, \mathrm{e}^{-\varepsilon}(1-\delta-\alpha)\right\} \tag{4}$$

for $0 \leq \alpha \leq 1$, which is a trade-off function. Figure 3 shows the graph of this function and its evident symmetry. The following result is adapted from Wasserman and Zhou (2010).

Proposition 3 (Wasserman and Zhou (2010))**.** *A mechanism M is (ε, δ)-DP if and only if M is $f_{\varepsilon,\delta}$-DP.*

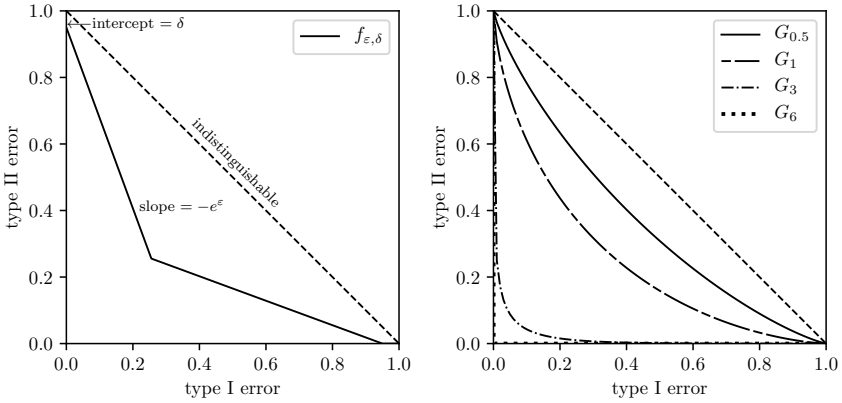

Fig. 3: Left: $f_{\varepsilon,\delta}$ is a piecewise linear function and is symmetric with respect to the line $y = x$. It has (nontrivial) slopes $-\mathrm{e}^{\pm\varepsilon}$ and intercepts $1-\delta$. Right: Trade-off functions of unit-variance Gaussian distributions with different means. The case of $\mu = 0.5$ is reasonably private, $\mu = 1$ is borderline private, and $\mu = 3$ is basically non-private: an adversary can control type I and type II errors simultaneously at only 0.07. In the case of $\mu = 6$ (almost coincides with the axes), the two errors both can be as small as 0.001.

2.2. Gaussian Differential Privacy

This subsection introduces a parametric family of f-DP guarantees, where f is the trade-off function of two normal distributions. We refer to this specialization as Gaussian differential privacy (GDP). GDP enjoys many desirable properties that lead to its central

role in this paper. Among others, we can now precisely define the trade-off function with a single parameter. To define this notion, let

$$G_\mu := T\big(\mathcal{N}(0,1), \mathcal{N}(\mu,1)\big)$$

for $\mu \geq 0$. An explicit expression for the trade-off function G_μ reads

$$G_\mu(\alpha) = \Phi\big(\Phi^{-1}(1-\alpha) - \mu\big), \tag{5}$$

where Φ denotes the standard normal CDF. For completeness, we provide a proof of (5) in Appendix A. This trade-off function is decreasing in μ in the sense that $G_\mu \leqslant G_{\mu'}$ if $\mu \geq \mu'$. We now define GDP:

Definition 4. *A mechanism M is said to satisfy μ-Gaussian Differential Privacy (μ-GDP) if it is G_μ-DP. That is,*

$$T\big(M(S), M(S')\big) \geq G_\mu$$

for all neighboring datasets S and S'.

GDP has several attractive properties. First, this privacy definition is fully described by the single mean parameter of a unit-variance Gaussian distribution, which makes it easy to describe and interpret the privacy guarantees. For instance, one can see from the right panel of Figure 3 that $\mu \leq 0.5$ guarantees a reasonable amount of privacy, whereas if $\mu \geqslant 6$, almost nothing is being promised. Second, loosely speaking, GDP occupies a role among all hypothesis testing based notions of privacy that is similar to the role that the Gaussian distribution has among general probability distributions. We formalize this important point by proving central limit theorems for f-DP in Section 3, which, roughly speaking, says that f-DP converges to GDP under composition in the limit. Lastly, as shown in the remainder of this subsection, GDP *precisely* characterizes the Gaussian mechanism, one of the most fundamental building blocks of differential privacy.

Consider the problem of privately releasing a univariate statistic $\theta(S)$ of the dataset S. Define the sensitivity of θ as

$$\mathrm{sens}(\theta) = \sup_{S,S'} |\theta(S) - \theta(S')|,$$

where the supremum is over all neighboring datasets. The Gaussian mechanism adds Gaussian noise to the statistic θ in order to obscure whether θ is computed on S or S'. The following result shows that the Gaussian mechanism with noise properly scaled to the sensitivity of the statistic satisfies GDP.

Theorem 1. *Define the Gaussian mechanism that operates on a statistic θ as $M(S) = \theta(S) + \xi$, where $\xi \sim \mathcal{N}(0, \mathrm{sens}(\theta)^2/\mu^2)$. Then, M is μ-GDP.*

Proof of Theorem 1. Recognizing that $M(S), M(S')$ are normally distributed with means $\theta(S), \theta(S')$, respectively, and common variance $\sigma^2 = \mathrm{sens}(\theta)^2/\mu^2$, we get

$$T\big(M(S), M(S')\big) = T\big(\mathcal{N}(\theta(S), \sigma^2), \mathcal{N}(\theta(S'), \sigma^2)\big) = G_{|\theta(S)-\theta(S')|/\sigma}.$$

By the definition of sensitivity, $|\theta(S) - \theta(S')|/\sigma \le \mathrm{sens}(\theta)/\sigma = \mu$. Therefore, we get

$$T\big(M(S), M(S')\big) = G_{|\theta(S)-\theta(S')|/\sigma} \geqslant G_\mu.$$

This completes the proof. □

As implied by the proof above, GDP offers the tightest possible privacy bound of the Gaussian mechanism. More precisely, the Gaussian mechanism in Theorem 1 satisfies

$$G_\mu(\alpha) = \inf_{\text{neighboring } S,S'} T\big(M(S), M(S')\big)(\alpha), \tag{6}$$

where the infimum is (asymptotically) achieved at the two neighboring datasets such that $|\theta(S)-\theta(S')| = \mathrm{sens}(\theta)$ *irrespective* of the type I error α. As such, the characterization by GDP is precise in the pointwise sense. In contrast, the right-hand side of (6) in general is not necessarily a convex function of α and, in such case, is not a trade-off function according to Proposition 1. This nice property of Gaussian mechanism is related to the log-concavity of Gaussian distributions. See Proposition A.3 for a detailed treatment of log-concave distributions.

2.3. Post-Processing and the Informativeness of f-DP

Intuitively, a data analyst cannot make a statistical analysis more disclosive only by processing the output of the mechanism M. This is called the post-processing property, a natural requirement that any notion of privacy, including our definition of f-DP, should satisfy.

To formalize this point for f-DP, denote by $\mathrm{Proc} : Y \to Z$ a (randomized) algorithm that maps the input $M(S) \in Y$ to some space Z, yielding a new mechanism that we denote by $\mathrm{Proc} \circ M$. The following result confirms the post-processing property of f-DP.

Proposition 4. *If a mechanism M is f-DP, then its post-processing $\mathrm{Proc} \circ M$ is also f-DP.*

Proposition 4 is a consequence of the following lemma. Let $\mathrm{Proc}(P)$ be the probability distribution of $\mathrm{Proc}(\zeta)$ with ζ drawn from P. Define $\mathrm{Proc}(Q)$ likewise.

lemma 1. *For any two distributions P and Q, we have $T\big(\mathrm{Proc}(P), \mathrm{Proc}(Q)\big) \geqslant T(P, Q)$.*

This lemma means that post-processed distributions can only become more difficult to tell apart than the original distributions from the perspective of trade-off functions. While the same property holds for many divergence based measures of indistinguishability such as the Rényi divergences used by the concentrated differential privacy family of definitions (Dwork and Rothblum, 2016; Bun and Steinke, 2016; Mironov, 2017; Bun et al., 2018a), a consequence of the following theorem is that trade-off functions offer the most informative measure among all. This remarkable inverse of Lemma 1 is due to Blackwell (see also Theorem 2.5 in Kairouz et al. (2017)).

Theorem 2 (Blackwell (1950), Theorem 10)**.** *Let P, Q be probability distributions on Y and P', Q' be probability distributions on Z. The following two statements are equivalent:*

(a) $T(P, Q) \leqslant T(P', Q')$.

(b) There exists a randomized algorithm $\mathrm{Proc} : Y \to Z$ *such that* $\mathrm{Proc}(P) = P', \mathrm{Proc}(Q) = Q'$.

To appreciate the implication of this theorem, we begin by observing that post-processing induces an order on pairs of distributions, which is called the Blackwell order (see, e.g., Raginsky (2011)). Specifically, if the above condition (b) holds, then we write $(P, Q) \preceq_{\text{Blackwell}} (P', Q')$ and interpret this as "(P, Q) is easier to distinguish than (P', Q') in the Blackwell sense". Similarly, when $T(P, Q) \leqslant T(P', Q')$, we write $(P, Q) \preceq_{\text{tradeoff}} (P', Q')$ and interpret this as "(P, Q) is easier to distinguish than (P', Q') in the testing sense". In general, any privacy measure used in defining a privacy notion induces an order $\preceq$ on pairs of distributions. Assuming the post-processing property for the privacy notion, the induced order $\preceq$ must be consistent with $\preceq_{\text{Blackwell}}$. Concretely, we denote by $\mathrm{Ineq}(\preceq) = \{(P, Q; P', Q') : (P, Q) \preceq (P', Q')\}$ the set of all comparable pairs of the order $\preceq$. As is clear, a privacy notion satisfies the post-processing property if and only if the induced order $\preceq$ satisfies $\mathrm{Ineq}(\preceq) \supseteq \mathrm{Ineq}(\preceq_{\text{Blackwell}})$.

Therefore, for any reasonable privacy notion, the set $\mathrm{Ineq}(\preceq)$ must be large enough to contain $\mathrm{Ineq}(\preceq_{\text{Blackwell}})$. However, it is also desirable to have a not too large $\mathrm{Ineq}(\preceq)$. For example, consider the privacy notion based on a trivial divergence D_0 with $D_0(P\|Q) \equiv 0$ for any P, Q. Note that $\mathrm{Ineq}(\preceq_{D_0})$ is the largest possible and, meanwhile, it is not informative at all in terms of measuring the indistinguishability of two distributions.

The argument above suggests that going from the "minimal" order $\mathrm{Ineq}(\preceq_{\text{Blackwell}})$ to the "maximal" order $\mathrm{Ineq}(\preceq_{D_0})$ would lead to information loss. Remarkably, f-DP is the most informative differential privacy notion from this perspective because its induced order $\preceq_{\text{tradeoff}}$ satisfies $\mathrm{Ineq}(\preceq_{\text{tradeoff}}) = \mathrm{Ineq}(\preceq_{\text{Blackwell}})$. In stark contrast, this is not true for the order induced by other popular privacy notions such as Rényi differential privacy and (ε, δ)-DP. We prove this claim in Appendix B and further justify the informativeness of f-DP by providing general tools that can losslessly convert f-DP guarantees into divergence based privacy guarantees.

2.4. A Primal-Dual Perspective

In this subsection, we show that f-DP is equivalent to an infinite *collection* of (ε, δ)-DP guarantees via the convex conjugate of the trade-off function. As a consequence of this, we can view f-DP as the *primal* privacy representation and, accordingly, its *dual* representation is the collection of (ε, δ)-DP guarantees. Taking this powerful viewpoint, many results from the large body of (ε, δ)-DP work can be carried over to f-DP in a seamless fashion. In particular, this primal-dual perspective is crucial to our analysis of "privacy amplification by subsampling" in Section 4. All proofs are deferred to Appendix A.

First, we present the result that converts a collection of (ε, δ)-DP guarantees into an f-DP guarantee. This result is self-evidence and its proof is, therefore, omitted.

Proposition 5 (Dual to Primal)**.** *Let I be an arbitrary index set such that each $i \in I$ is associated with $\varepsilon_i \in [0, \infty)$ and $\delta_i \in [0, 1]$. A mechanism is $(\varepsilon_i, \delta_i)$-DP for all $i \in I$ if and only if it is f-DP with*

$$f = \sup_{i \in I} f_{\varepsilon_i, \delta_i}.$$

This proposition follows easily from the equivalence of (ε, δ)-DP and $f_{\varepsilon,\delta}$-DP. We remark that the function f constructed above remains a symmetric trade-off function.

The more interesting direction is to convert f-DP into a collection of (ε, δ)-DP guarantees. Recall that the convex conjugate of a function g defined on $(-\infty, \infty)$ is defined as

$$g^*(y) = \sup_{-\infty<x<\infty} yx - g(x). \tag{7}$$

To define the conjugate of a trade-off function f, we extend its domain by setting $f(x) = \infty$ for $x < 0$ and $x > 1$. With this adjustment, the supremum is effectively taken over $0 \le x \le 1$.

Proposition 6 (Primal to Dual)**.** *For a symmetric trade-off function f, a mechanism is f-DP if and only if it is $\big(\varepsilon, \delta(\varepsilon)\big)$-DP for all $\varepsilon \geqslant 0$ with $\delta(\varepsilon) = 1 + f^*(-\mathrm{e}^{\varepsilon})$.*

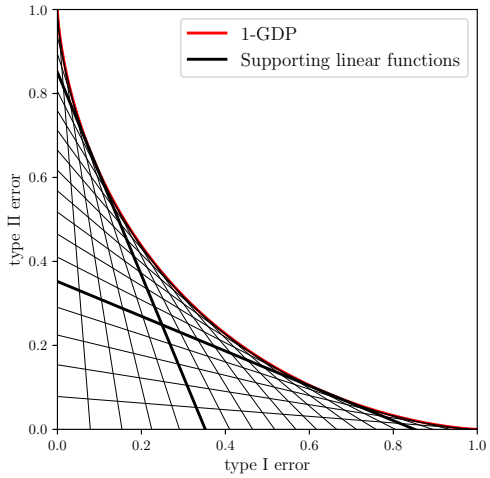

Fig. 4: Each $(\varepsilon, \delta(\varepsilon))$-DP guarantee corresponds to two supporting linear functions (symmetric to each other) to the trade-off function describing the complete f-DP guarantee. In general, characterizing a privacy guarantee using only a subset of (ε, δ)-DP guarantees (for example, only those with small δ) would result in information loss.

For example, taking $f = G_\mu$, the following corollary provides a lossless conversion from GDP to a collection of (ε, δ)-DP guarantees. This conversion is exact and, therefore, any other (ε, δ)-DP guarantee derived for the Gaussian mechanism is implied by this corollary. See Figure 4 for an illustration of this result.

Corollary 1. *A mechanism is μ-GDP if and only if it is $\big(\varepsilon, \delta(\varepsilon)\big)$-DP for all $\varepsilon \geqslant 0$, where*

$$\delta(\varepsilon) = \Phi\Big(-\frac{\varepsilon}{\mu} + \frac{\mu}{2}\Big) - \mathrm{e}^{\varepsilon}\Phi\Big(-\frac{\varepsilon}{\mu} - \frac{\mu}{2}\Big).$$

This corollary has appeared earlier in Balle and Wang (2018). Along this direction, Balle et al. (2018) further proposed "privacy profile", which in essence corresponds to an

infinite collection of (ε, δ). The notion of privacy profile mainly serves as an analytical tool in Balle et al. (2018).

The primal-dual perspective provides a useful tool through which we can bridge the two privacy definitions. In some cases, it is easier to work with f-DP by leveraging the interpretation and informativeness of trade-off functions, as seen from the development of composition theorems for f-DP in Section 3. Meanwhile, (ε, δ)-DP is more convenient to work with in the cases where the lower complexity of two parameters ε, δ is helpful, for example, in the proof of the privacy amplification by subsampling theorem for f-DP. In short, our approach in Section 4 is to first work in the dual world and use existing subsampling theorems for (ε, δ)-DP, and then convert the results back to f-DP using a slightly more advanced version of Proposition 6.

2.5. Group Privacy

The notion of f-DP can be extended to address privacy of a *group* of individuals, and a question of interest is to quantify how privacy degrades as the group size grows. To set up the notation, we say that two datasets S, S' are k-neighbors (where $k \geq 2$ is an integer) if there exist datasets $S = S_0, S_1, \ldots, S_k = S'$ such that S_i and S_{i+1} are neighboring or identical for all $i = 0, \ldots, k-1$. Equivalently, S, S' are k-neighbors if they differ by at most k individuals. Accordingly, a mechanism M is said to be f-DP for *groups of size* k if

$$T\big(M(S), M(S')\big) \geqslant f$$

for all k-neighbors S and S'.

In the following theorem, we use $h^{\circ k}$ to denote the k-fold iterative composition of a function h. For example, $h^{\circ 1} = h$ and $h^{\circ 2}(x) = h(h(x))$.

Theorem 3. *If a mechanism is f-DP, then it is $\big[1 - (1-f)^{\circ k}\big]$-DP for groups of size k. In particular, if a mechanism is μ-GDP, then it is $k\mu$-GDP for groups of size k.*

For completeness, $1 - (1-f)^{\circ k}$ is a trade-off function and, moreover, remains symmetric if f is symmetric. These two facts and Theorem 3 are proved in Appendix A. As revealed in the proof, the privacy bound $1 - (1-f)^{\circ k}$ in general cannot be improved, thereby showing that the group operation in the f-DP framework is *closed* and *tight*. In addition, it is easy to see that $1 - (1-f)^{\circ k} \leqslant 1 - (1-f)^{\circ (k-1)}$ by recognizing that the trade-off function f satisfies $1 - f(x) \geqslant x$. This is consistent with the intuition that detecting changes in groups of k individuals becomes easier as the group size increases.

As an interesting consequence of Theorem 3, the group privacy of ε-DP in the limit corresponds to the trade-off function of two Laplace distributions. Recall that the density of $\mathrm{Lap}(\mu, b)$ is $\frac{1}{2b}\mathrm{e}^{-|x-\mu|/b}$.

Proposition 7. *Fix $\mu \geq 0$ and set $\varepsilon = \mu/k$. As $k \to \infty$, we have*

$$1 - (1 - f_{\varepsilon,0})^{\circ k} \to T\big(\mathrm{Lap}(0,1), \mathrm{Lap}(\mu, 1)\big).$$

The convergence is uniform over $[0, 1]$.

Two remarks are in order. First, $T\big(\mathrm{Lap}(0,1), \mathrm{Lap}(\mu,1)\big)$ is not equal to $f_{\varepsilon,\delta}$ for any ε, δ and, therefore, (ε, δ)-DP is not expressive enough to measure privacy under the

group operation. Second, the approximation in this theorem is very accurate even for small k. For example, for $\mu = 1, k = 4$, the function $1 - (1 - f_{\varepsilon,0})^{\circ k}$ is within 0.005 of $T\big(\mathrm{Lap}(0,1), \mathrm{Lap}(\mu,1)\big)$ uniformly over $[0,1]$. The proof of Proposition 7 is deferred to Appendix A.

3. Composition and Limit Theorems

Imagine that an analyst performs a sequence of analyses on a private dataset, in which each analysis is informed by prior analyses on the same dataset. Provided that every analysis alone is private, the question is whether all analyses collectively are private, and if so, how the privacy degrades as the number of analyses increases, namely under composition. It is essential for a notion of privacy to gracefully handle composition, without which the privacy analysis of complex algorithms would be almost impossible.

Now, we describe the composition of two mechanisms. For simplicity, this section writes X for the space of datasets and abuse notation by using n to refer to the number of mechanisms in composition (the use of n is consistent with the literature on central limit theorems). Let $M_1 : X \to Y_1$ be the first mechanism and $M_2 : X \times Y_1 \to Y_2$ be the second mechanism. In brief, M_2 takes as input the output of the first mechanism M_1 in addition to the dataset. With the two mechanisms in place, the joint mechanism $M : X \to Y_1 \times Y_2$ is defined as

$$M(S) = (y_1, M_2(S, y_1)), \tag{8}$$

where $y_1 = M_1(S)$. Roughly speaking, the distribution of $M(S)$ is constructed from the marginal distribution of $M_1(S)$ on Y_1 and the conditional distribution of $M_2(S, y_1)$ on Y_2 given $M_1(S) = y_1$. The composition of more than two mechanisms follows recursively. In general, given a sequence of mechanisms $M_i : X \times Y_1 \times \cdots \times Y_{i-1} \to Y_i$ for $i = 1, 2, \ldots, n$, we can recursively define the joint mechanism as their composition:

$$M : X \to Y_1 \times \cdots \times Y_n.$$

Put differently, $M(S)$ can be interpreted as the trajectory of a Markov chain whose initial distribution is given by $M_1(S)$ and the transition kernel $M_i(S, \cdots)$ at each step.

Using the language above, the goal of this section is to relate the privacy loss of M to that of the n mechanisms $M_1, \ldots, M_n$ in the f-DP framework. In short, Section 3.1 develops a general composition theorem for f-DP. In Sections 3.2, we identify a central limit theorem phenomenon of composition in the f-DP framework, which can be used as an approximation tool, just like we use the central limit theorem for random variables. This approximation is extended to and improved for (ε, δ)-DP in Section 3.3.

3.1. A General Composition Theorem

The main thrust of this subsection is to demonstrate that the composition of private mechanisms is closed and tight in the f-DP framework. This result is formally stated in Theorem 4, which shows that the composed mechanism remains f-DP with the trade-off function taking the form of a certain product. To define the product, consider two trade-off functions f and g that are given as $f = T(P, Q)$ and $g = T(P', Q')$ for some probability distributions P, P', Q, Q'.

Definition 5. *The tensor product of two trade-off functions $f = T(P, Q)$ and $g = T(P', Q')$ is defined as*

$$f \otimes g := T(P \times P', Q \times Q').$$

Throughout the paper, write $f \otimes g(\alpha)$ for $(f \otimes g)(\alpha)$, and denote by $f^{\otimes n}$ the n-fold tensor product of f. The well-definedness of $f^{\otimes n}$ rests on the associativity of the tensor product, which we will soon illustrate.

By definition, $f \otimes g$ is also a trade-off function. Nevertheless, it remains to be shown that the tensor product is well-defined: that is, the definition is independent of the choice of distributions used to represent a trade-off function. More precisely, assuming $f = T(P, Q) = T(\tilde{P}, \tilde{Q})$ for some distributions $\tilde{P}, \tilde{Q}$, we need to ensure that

$$T(P \times P', Q \times Q') = T(\tilde{P} \times P', \tilde{Q} \times Q').$$

We defer the proof of this intuitive fact to Appendix C. Below we list some other useful properties of the tensor product of trade-off functions, whose proofs are placed in Appendix D.

(a) The product $\otimes$ is commutative and associative.

(b) If $g_1 \geqslant g_2$, then $f \otimes g_1 \geqslant f \otimes g_2$.

(c) $f \otimes \mathrm{Id} = \mathrm{Id} \otimes f = f$, where the identity trade-off function $\mathrm{Id}(x) = 1 - x$ for $0 \leq x \leq 1$.

(d) $(f \otimes g)^{-1} = f^{-1} \otimes g^{-1}$. See the definition of inverse in (3).

Note that Id is the trade-off function of two identical distributions. Property 4 implies that when f, g are symmetric trade-off functions, their tensor product $f \otimes g$ is also symmetric.

Now we state the main theorem of this subsection. Its proof is given in Appendix C.

Theorem 4. *Let $M_i(\cdot, y_1, \cdots, y_{i-1})$ be f_i-DP for all $y_1 \in Y_1, \ldots, y_{i-1} \in Y_{i-1}$. Then the n-fold composed mechanism $M : X \to Y_1 \times \cdots \times Y_n$ is $f_1 \otimes \cdots \otimes f_n$-DP.*

This theorem shows that the composition of mechanisms remains f-DP or, put differently, composition is closed in the f-DP framework. Moreover, the privacy bound $f_1 \otimes \cdots \otimes f_n$ in Theorem 4 is *tight* in the sense that it cannot be improved in general. To see this point, consider the case where the second mechanism completely ignores the output of the first mechanism. In that case, the composition obeys

$$\begin{aligned} T\big(M(S), M(S')\big) &= T\big(M_1(S) \times M_2(S), M_1(S') \times M_2(S')\big) \\ &= T\big(M_1(S), M_1(S')\big) \otimes T\big(M_2(S), M_2(S')\big). \end{aligned}$$

Next, taking neighboring datasets such that $T\big(M_1(S), M_1(S')\big) = f_1$ and $T\big(M_2(S), M_2(S')\big) = f_2$, one concludes that $f_1 \otimes f_2$ is the tightest possible bound on the two-fold composition. For comparison, the advanced composition theorem for (ε, δ)-DP does not admit a single pair of optimal parameters ε, δ (Dwork et al., 2010). In particular, no pair of ε, δ can exactly capture the privacy of the composition of (ε, δ)-DP mechanisms. See Section 3.3 and Figure 5 for more elaboration.

In the case of GDP, composition enjoys a simple and convenient formulation due to the identity

$$G_{\mu_1} \otimes G_{\mu_2} \otimes \cdots \otimes G_{\mu_n} = G_{\mu},$$

where $\mu = \sqrt{\mu_1^2 + \cdots + \mu_n^2}$. This formula is due to the rotational invariance of Gaussian distributions with identity covariance. We provide the proof in Appendix D. The following corollary formally summarizes this finding.

Corollary 2. *The n-fold composition of μ_i-GDP mechanisms is $\sqrt{\mu_1^2 + \cdots + \mu_n^2}$-GDP.*

On a related note, the pioneering work Kairouz et al. (2017) is the first to take the hypothesis testing viewpoint in the study of privacy composition and to use Blackwell's theorem as an analytic tool therein. In particular, the authors offered a composition theorem for (ε, δ)-DP that improves on the advanced composition theorem (Dwork et al., 2010). Following this work, Murtagh and Vadhan (2016) provided a self-contained proof by essentially proving the "(ε, δ) special case" of Blackwell's theorem. In contrast, our novel proof of Theorem 4 only makes use of the Neyman–Pearson lemma, thereby circumventing the heavy machinery of Blackwell's theorem. This simple proof better illuminates the essence of the composition theorem.

3.2. Central Limit Theorems for Composition

In this subsection, we identify a central limit theorem type phenomenon of composition in the f-DP framework. Our main results (Theorem 5 and Theorem 6), roughly speaking, show that trade-off functions corresponding to small privacy leakage accumulate to G_μ for some μ under composition. Equivalently, the privacy of the composition of many "very private" mechanisms is best measured by GDP in the limit. This identifies GDP as the focal privacy definition among the family of f-DP privacy guarantees, including (ε, δ)-DP. More precisely, *all* privacy definitions that are based on a hypothesis testing formulation of "indistinguishability" converge to the guarantees of GDP in the limit of composition. We remark that Sommer et al. (2018) proved a conceptually related central limit theorem for random variables corresponding to the privacy loss. This theorem is used to reason about the non-adaptive composition for (ε, δ)-DP. In contrast, our central limit theorem is concerned with the optimal hypothesis testing trade-off functions for the composition theorem. Moreover, our theorem is applicable in the setting of composition, where each mechanism is informed by prior interactions with the same database.

From a computational viewpoint, these limit theorems yield an efficient method of approximating the composition of general f-DP mechanisms. This is very appealing for analyzing the privacy properties of algorithms that are comprised of many building blocks in a sequence. For comparison, the exact computation of privacy guarantees under composition can be computationally hard (Murtagh and Vadhan, 2016) and, thus, tractable approximations are important. Using our central limit theorems, the computation of the exact overall privacy guarantee $f_1 \otimes \cdots \otimes f_n$ in Theorem 4 can be reduced to the evaluation of a single mean parameter μ in a GDP guarantee. We give an exemplary application of this powerful technique in Section 5.

Explicitly, the mean parameter μ in the approximation depends on certain functionals

of the trade-off functions:

$$\mathrm{kl}(f) := -\int_0^1 \log|f'(x)|\,\mathrm{d}x, \quad \kappa_2(f) := \int_0^1 \log^2|f'(x)|\,\mathrm{d}x$$
$$\kappa_3(f) := \int_0^1 \big|\log|f'(x)|\big|^3\,\mathrm{d}x, \quad \bar{\kappa}_3(f) := \int_0^1 \big|\log|f'(x)| + \mathrm{kl}(f)\big|^3\,\mathrm{d}x.$$

All of these functionals take values in $[0, +\infty]$, and the last is defined for f such that $\mathrm{kl}(f) < \infty$. In essence, these functionals are calculating moments of the log-likelihood ratio of P and Q such that $f = T(P, Q)$. In particular, all of these functionals are 0 if $f(x) = \mathrm{Id}(x) = 1 - x$, which corresponds to zero privacy leakage. As its name suggests, $\mathrm{kl}(f)$ is the Kullback–Leibler (KL) divergence of P and Q and, therefore, $\mathrm{kl}(f) \geq 0$. Detailed elaboration on these functionals is deferred to Appendix D.

In the following theorem, $\mathbf{kl}$ denotes the vector $\big(\mathrm{kl}(f_1), \ldots, \mathrm{kl}(f_n)\big)$ and $\boldsymbol{\kappa_2}, \boldsymbol{\kappa_3}, \bar{\boldsymbol{\kappa}}_{\boldsymbol{3}}$ are defined similarly; in addition, $\|\cdot\|_1$ and $\|\cdot\|_2$ are the ℓ_1 and ℓ_2 norms, respectively. Its proof can be found in Appendix D

Theorem 5. *Let $f_1, \ldots, f_n$ be symmetric trade-off functions such that $\kappa_3(f_i) < \infty$ for all $1 \leq i \leq n$. Denote*

$$\mu := \frac{2\|\mathbf{kl}\|_1}{\sqrt{\|\boldsymbol{\kappa_2}\|_1 - \|\mathbf{kl}\|_2^2}} \quad \textit{and} \quad \gamma := \frac{0.56\|\bar{\boldsymbol{\kappa}}_{\boldsymbol{3}}\|_1}{\big(\|\boldsymbol{\kappa_2}\|_1 - \|\mathbf{kl}\|_2^2\big)^{3/2}}$$

and assume $\gamma < \frac{1}{2}$. Then, for all $\alpha \in [\gamma, 1-\gamma]$, we have

$$G_\mu(\alpha + \gamma) - \gamma \leqslant f_1 \otimes f_2 \otimes \cdots \otimes f_n(\alpha) \leqslant G_\mu(\alpha - \gamma) + \gamma. \tag{9}$$

From a technical viewpoint, Theorem 5 can be thought of as a Berry–Esseen type central limit theorem. Loosely speaking, the lower bound in (9) shows that the composition of f_i-DP mechanisms for $i = 1, \ldots, n$ is approximately μ-GDP and, in addition, the upper bound demonstrates that the tightness of this approximation is specified by γ. In the case where all f_i are equal to some $f \neq \mathrm{Id}$, the theorem reveals that the composition becomes blatantly non-private as $n \to \infty$ because $\mu \asymp \sqrt{n} \to \infty$. More interesting applications of the theorem, however, are cases where each f_i is close to the "perfect privacy" trade-off function Id such that collectively μ is convergent and γ vanishes as $n \to \infty$ (see the example in Section 5). For completeness, the condition $\kappa_3(f_i) < \infty$ (which implies that the other three functionals are also finite) for the use of this theorem excludes the case where $f_i(0) < 1$, in particular, $f_{\varepsilon,\delta}$ in (ε, δ)-DP with $\delta > 0$. We introduce an easy and general technique in Section 3.3 to deal with this issue.

Next, we present an asymptotic version of Theorem 5 for composition of f-DP mechanisms. In analog to classical central limit theorems, below we consider a triangular array of mechanisms $\{M_{n1}, \ldots, M_{nn}\}_{n=1}^{\infty}$, where M_{ni} is f_{ni}-DP for $1 \leq i \leq n$. As with Theorem 5, the proof of Theorem 6 is relegated to Appendix D.

Theorem 6. *Let $\{f_{ni} : 1 \leqslant i \leqslant n\}_{n=1}^{\infty}$ be a triangular array of symmetric trade-off functions and assume the following limits for some constants $K \geq 0$ and $s > 0$ as $n \to \infty$:*

1. $\sum_{i=1}^{n} \mathrm{kl}(f_{ni}) \to K$;
2. $\max_{1 \leqslant i \leqslant n} \mathrm{kl}(f_{ni}) \to 0$;
3. $\sum_{i=1}^{n} \kappa_2(f_{ni}) \to s^2$;
4. $\sum_{i=1}^{n} \kappa_3(f_{ni}) \to 0$.

Then, we have

$$\lim_{n\to\infty} f_{n1} \otimes f_{n2} \otimes \cdots \otimes f_{nn}(\alpha) = G_{2K/s}(\alpha)$$

uniformly for all $\alpha \in [0, 1]$.

Taken together, this theorem and Theorem 4 amount to saying that the composition $M_{n1} \otimes \ldots \otimes M_{nn}$ is asymptotically $2K/s$-GDP. In fact, this asymptotic version is a consequence of Theorem 5 as one can show $\mu \to 2K/s$ and $\gamma \to 0$ for the triangular array of symmetric trade-off functions. This central limit theorem implies that GDP is the *only* parameterized family of trade-off functions that can faithfully represent the effects of composition. In contrast, neither ε- nor (ε, δ)-DP can losslessly be tracked under composition—the parameterized family of functions $f_{\varepsilon,\delta}$ cannot represent the trade-off function that results from the limit under composition.

The conditions for use of this theorem are reminiscent of Lindeberg's condition in the central limit theorem for independent random variables. The proper scaling of the trade-off functions is that both $\mathrm{kl}(f_{ni})$ and $\kappa_2(f_{ni})$ are of order $O(1/n)$ for most $1 \leq i \leq n$. As a consequence, the cumulative effects of the moment functionals are bounded. Furthermore, as with Lindeberg's condition, the second condition in Theorem 6 requires that no single mechanism has a significant contribution to the composition in the limit.

In passing, we remark that K and s satisfy the relationship $s = \sqrt{2K}$ in all examples of the application of Theorem 6 in this paper, including Theorem 7 and Theorem 11 as well as their corollaries. As such, the composition is asymptotically s-GDP. A proof of this interesting observation or the construction of a counterexample is left for future work.

3.3. Composition of (ε, δ)-DP: Beating Berry–Esseen

Now, we extend central limit theorems to (ε, δ)-DP. As shown by Proposition 3, (ε, δ)-DP is equivalent to $f_{\varepsilon,\delta}$-DP and, therefore, it suffices to approximate the trade-off function $f_{\varepsilon_1,\delta_1} \otimes \cdots \otimes f_{\varepsilon_n,\delta_n}$ by making use of the composition theorem for f-DP mechanisms. As pointed out in Section 3.2, however, the moment conditions required in the two central limit theorems (Theorems 5 and 6) exclude the case where $\delta_i > 0$.

To overcome the difficulty caused by a nonzero δ, we start by observing the useful fact that

$$f_{\varepsilon,\delta} = f_{\varepsilon,0} \otimes f_{0,\delta}. \tag{10}$$

This decomposition, along with the commutative and associative properties of the tensor product, shows

$$f_{\varepsilon_1,\delta_1} \otimes \cdots \otimes f_{\varepsilon_n,\delta_n} = \big(f_{\varepsilon_1,0} \otimes \cdots \otimes f_{\varepsilon_n,0}\big) \otimes \big(f_{0,\delta_1} \otimes \cdots \otimes f_{0,\delta_n}\big).$$

This identity allows us to work on the ε part and δ part separately. In short, the ε part $f_{\varepsilon_1,0} \otimes \cdots \otimes f_{\varepsilon_n,0}$ now can be approximated by $G_{\sqrt{\varepsilon_1^2+\cdots+\varepsilon_n^2}}$ by invoking Theorem 6. For the δ part, we can iteratively apply the rule

$$f_{0,\delta_1} \otimes f_{0,\delta_2} = f_{0,1-(1-\delta_1)(1-\delta_2)} \tag{11}$$

to obtain $f_{0,\delta_1} \otimes \cdots \otimes f_{0,\delta_n} = f_{0,1-(1-\delta_1)(1-\delta_2)\cdots(1-\delta_n)}$. This rule is best seen via the interesting fact that $f_{0,\delta}$ is the trade-off function of shifted uniform distributions $T\big(U[0,1], U[\delta, 1+\delta]\big)$.

Now, a central limit theorem for (ε, δ)-DP is just a stone's throw away. In what follows, the privacy parameters ε and δ are arranged in a triangular array $\{(\varepsilon_{ni}, \delta_{ni}) : 1 \leqslant i \leqslant n\}_{n=1}^{\infty}$.

Theorem 7. *Assume*

$$\sum_{i=1}^{n} \varepsilon_{ni}^2 \to \mu^2, \quad \max_{1 \leqslant i \leqslant n} \varepsilon_{ni} \to 0, \quad \sum_{i=1}^{n} \delta_{ni} \to \delta, \quad \max_{1 \leqslant i \leqslant n} \delta_{ni} \to 0$$

for some nonnegative constants μ, δ as $n \to \infty$. Then, we have

$$f_{\varepsilon_{n1},\delta_{n1}} \otimes \cdots \otimes f_{\varepsilon_{nn},\delta_{nn}} \to G_\mu \otimes f_{0,1-\mathrm{e}^{-\delta}}$$

uniformly over $[0,1]$ as $n \to \infty$.

The proof of this theorem is provided in Appendix D. The assumptions concerning $\{\delta_{ni}\}$ give rise to $1 - (1-\delta_{n1})(1-\delta_{n2}) \cdots (1-\delta_{nn}) \to 1 - \mathrm{e}^{-\delta}$. In general, tensoring with $f_{0,\delta}$ is equivalent to scaling the graph of the trade-off function f toward the origin by a factor of $1-\delta$. This property is specified by the following formula, and we leave its proof to Appendix D:

$$f \otimes f_{0,\delta}(\alpha) = \begin{cases} (1-\delta) \cdot f(\frac{\alpha}{1-\delta}), & 0 \leqslant \alpha \leqslant 1-\delta \\ 0, & 1-\delta \leqslant \alpha \leqslant 1. \end{cases} \tag{12}$$

In particular, $f \otimes f_{0,\delta}$ is symmetric if f is symmetric. Note that (10) and (11) can be deduced by the formula above.

This theorem interprets the privacy level of the composition using Gaussian and uniform distributions. Explicitly, the theorem demonstrates that, based on the released information of the composed mechanism, distinguishing between any neighboring datasets is at least as hard as distinguishing between the following two bivariate distributions:

$$\mathcal{N}(0,1) \times U[0,1] \text{ versus } \mathcal{N}(\mu,1) \times U[1-\mathrm{e}^{-\delta}, 2-\mathrm{e}^{-\delta}].$$

We note that for small δ, $\mathrm{e}^{-\delta} \approx 1-\delta$. So $U[1-\mathrm{e}^{-\delta}, 2-\mathrm{e}^{-\delta}] \approx U[\delta, 1+\delta]$.

This approximation of the tensor product $f_{\varepsilon_{n1},\delta_{n1}} \otimes \cdots \otimes f_{\varepsilon_{nn},\delta_{nn}}$ using simple distributions is important from the viewpoint of computational complexity. Murtagh and Vadhan (2016) showed that, given a collection of $\{(\varepsilon_i, \delta_i)\}_{i=1}^n$, finding the smallest ε such that $f_{\varepsilon,\delta} \leqslant f_{\varepsilon_1,\delta_1} \otimes \cdots \otimes f_{\varepsilon_n,\delta_n}$ is #P-hard for any δ (#P is a complexity class that is "even harder than" NP; see, e.g., Ch. 9. of Arora and Barak (2009)). From the dual

perspective (see Section 2.4), this negative result is equivalent to the #P-hardness of evaluating the convex conjugate $\left(f_{\varepsilon_1,\delta_1} \otimes \cdots \otimes f_{\varepsilon_n,\delta_n}\right)^*$ at any point. For completeness, we remark that Murtagh and Vadhan (2016) provided an FPTAS (an approximation algorithm is called a fully polynomial-time approximation scheme (FPTAS) if its running time is polynomial in both the input size and the inverse of the relative approximation error; see, e.g., Ch. 8. of Vazirani (2013)) to approximately find the smallest ε in $O(n^3)$ time for a *single* δ. In comparison, Theorem 7 offers a *global* approximation of the tensor product in $O(n)$ time using a closed-form expression, subsequently enabling an analytical approximation of the smallest ε for each δ.

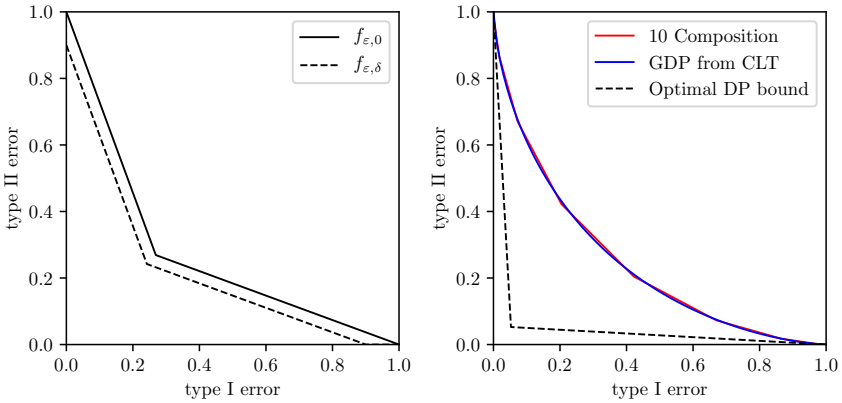

Fig. 5: Left: Tensoring with $f_{0,\delta}$ scales the graph towards the origin by a factor of $1-\delta$. Right: 10-fold composition of $(1/\sqrt{10}, 0)$-DP mechanisms, that is, $f_{\varepsilon,0}^{\otimes n}$ with $n = 10, \varepsilon = 1/\sqrt{n}$. The dashed curve corresponds to $\varepsilon = 2.89, \delta = 0.001$. These values are obtained by first setting $\delta = 0.001$ and finding the smallest ε such that the composition is (ε, δ)-DP. Note that the central limit theorem approximation to the true trade-off curve is almost perfect, whereas the tightest possible approximation via (ε, δ)-DP is substantially looser.

That being said, Theorem 7 remains silent on the approximation error in applications with a moderately large number of (ε, δ)-DP mechanisms. Alternatively, we can apply Theorem 5 to obtain a non-asymptotic normal approximation to $f_{\varepsilon_1,0} \otimes \cdots \otimes f_{\varepsilon_n,0}$ and use γ to specify the approximation error. It can be shown that $\gamma = O(1/\sqrt{n})$ under mild conditions (Corollary D.7). This bound, however, is not sharp enough for tight privacy guarantees if n is not too large (note that $1/\sqrt{n} \approx 0.14$ if $n = 50$, for which exact computation is already challenging, if possible at all). Surprisingly, the following theorem establishes a $O(1/n)$ bound, thereby "beating" the classical Berry–Esseen bound. The proof is given in Appendix D.

Theorem 8. *Fix $\mu > 0$ and let $\varepsilon = \mu/\sqrt{n}$. There is a constant $c > 0$ that only depends on μ satisfying*

$$G_\mu\left(\alpha + \tfrac{c}{n}\right) - \tfrac{c}{n} \leqslant f_{\varepsilon,0}^{\otimes n}(\alpha) \leqslant G_\mu\left(\alpha - \tfrac{c}{n}\right) + \tfrac{c}{n}$$

for all $n \geqslant 1$ and $c/n \leq \alpha \leq 1 - c/n$.

As with Theorem 7, this theorem can be extended to approximate DP ($\delta \neq 0$) by

making use of the decomposition (10). Our simulation studies suggest that $c \approx 0.1$ for $\mu = 1$, which is best illustrated in the right panel of Figure 5. Despite a fairly small $n = 10$, the difference between G_1 and its target $f_{\varepsilon,0}^{\otimes n}$ is less than 0.013 in the pointwise sense. For completeness, it is worthwhile mentioning that a better approximation can be obtained by using the Edgeworth expansion in place of the central limit theorem (Zheng et al., 2020). Interestingly, our numerical evidence suggests the same $O(1/n)$ rate under inhomogeneous composition, provided that $\varepsilon_1, \ldots, \varepsilon_n$ are roughly the same size. A formal proof, or even a quantitative statement of this observation, constitutes an interesting problem for future investigation.

In closing this section, we highlight some novelties in the proof of Theorem 8. Denoting $p_\varepsilon = \frac{1}{1+e^\varepsilon}$ and $q_\varepsilon = \frac{e^\varepsilon}{1+e^\varepsilon}$, Kairouz et al. (2017) presented a very useful expression (rephrased in our framework):

$$f_{\varepsilon,0}^{\otimes n} = T\big(B(n, p_\varepsilon), B(n, q_\varepsilon)\big),$$

where $B(n, p)$ denotes the binomial distribution with n trials and success probability p. However, directly approximating $f_{\varepsilon,0}^{\otimes n}$ through these two binomial distributions is unlikely to yield an $O(1/n)$ bound because the Berry–Esseen bound is rate-optimal for binomial distributions. Our analysis, instead, rests crucially on a certain smoothing effect that comes for free in testing between the two distributions. It is analogous to the continuity correction for normal approximations to binomial probabilities. See the technical details in Appendix D.

4. Amplifying Privacy by Subsampling

Subsampling is often used prior to a private mechanism M as a way to *amplify* privacy guarantees. Specifically, we can construct a smaller dataset $\tilde{S}$ by flipping a fair coin for each individual in the original dataset S to decide whether the individual is included in $\tilde{S}$. This subsampling scheme roughly shrinks the dataset by half and, therefore, we would expect that the induced mechanism applied to $\tilde{S}$ is about twice as private as the original mechanism M. Intuitively speaking, this privacy amplification is due to the fact that every individual enjoys perfect privacy if the individual is not included in the resulting dataset $\tilde{S}$, which happens with probability 50%.

The claim above was first formalized in Kasiviswanathan et al. (2011) for (ε, δ)-DP. Such a privacy amplification property is, unfortunately, no longer true for the most natural previous relaxations of differential privacy aimed at recovering precise compositions (like concentrated differential privacy (CDP) (Dwork and Rothblum, 2016; Bun and Steinke, 2016)). Further modifications such as truncated CDP (Bun et al., 2018a) have been introduced primarily to remedy this deficiency of CDP—but at the cost of extra complexity in the definition. Other relaxations like Rényi differential privacy (Mironov, 2017) can be shown to satisfy a form of privacy amplification by subsampling, but both the analysis and the statement are complex (Wang et al., 2018).

In this section, we show that these obstacles can be overcome by our hypothesis testing based relaxation of differential privacy. Explicitly, our main result is a simple, general, and easy-to-interpret subsampling theorem for f-DP. Somewhat surprisingly, our theorem significantly improves on the classical subsampling theorem for privacy

amplification in the (ε, δ)-DP framework (Ullman, 2017). Note that this classical theorem continues to use (ε, δ)-DP to characterize the subsampled mechanism. However, (ε, δ)-DP is simply not expressive enough to capture the amplification of privacy.

4.1. A Subsampling Theorem

Given an integer $1 \le m \le n$ and a dataset S of n individuals, let $\texttt{Sample}_m(S)$ be a subset of S that is chosen uniformly at random among all the m-sized subsets of S. For a mechanism M defined on X^m, we call $M\big(\texttt{Sample}_m(S)\big)$ the subsampled mechanism, which takes as input an n-sized dataset. Formally, we use $M \circ \texttt{Sample}_m$ to denote this subsampled mechanism. To clear up any confusion, note that intermediate result $\texttt{Sample}_m(S)$ is not released and, in particular, this is different from the composition in Section 3.

In brief, our main theorem shows that the privacy bound of the subsampled mechanism in the f-DP framework is given by an operator acting on trade-off functions. To introduce this operator, write the convex combination $f_p := pf + (1-p)\mathrm{Id}$ for $0 \le p \le 1$, where $\mathrm{Id}(x) = 1 - x$. Note that the trade-off function f_p is asymmetric in general.

Definition 6. *For any $0 \le p \le 1$, define the operator C_p acting on trade-off functions as*

$$C_p(f) := \min\{f_p, f_p^{-1}\}^{**}.$$

We call C_p the p-sampling operator.

Above, the inverse f_p^{-1} is defined in (3). The biconjugate $\min\{f_p, f_p^{-1}\}^{**}$ is derived by applying the conjugate as defined in (7) twice to $\min\{f_p, f_p^{-1}\}$. For the moment, take for granted the fact that $C_p(f)$ is a symmetric trade-off function.

Now, we present the main theorem of this section. Section 4.2 is devoted to proving this result.

Theorem 9. *If M is f-DP on X^m, then the subsampled mechanism $M \circ \texttt{Sample}_m$ is $C_p(f)$-DP on X^n, where the sampling ratio $p = \frac{m}{n}$.*

Appreciating this theorem calls for a better understanding of the operator C_p. In effect, C_p performs a two-step transformation: symmetrization (taking the minimum of f_p and its inverse f_p^{-1}) and convexification (taking the largest convex lower envelope of $\min\{f_p, f_p^{-1}\}$). The convexification step is seen from convex analysis that the biconjugate h^{**} of any function h is the greatest convex lower bound of h. As such, $C_p(f)$ is convex and, with a bit more analysis, Proposition 1 ensures that $C_p(f)$ is indeed a trade-off function. As an aside, $C_p(f) \le \min\{f_p, f_p^{-1}\} \le f_p$. See Figure 6 for a graphical illustration.

Next, the following facts concerning the p-sampling operator qualitatively illustrate this privacy amplification phenomenon.

(a) If $0 \leqslant p \leqslant q \leqslant 1$ and f is symmetric, we have $f = C_1(f) \leqslant C_q(f) \leqslant C_p(f) \leqslant C_0(f) = \mathrm{Id}$. That is, as the sampling ratio declines from 1 to 0, the privacy guarantee interpolates monotonically between the original f and the perfect privacy guarantee Id. This monotonicity follows from the fact that $g \ge h$ is equivalent to $g^{-1} \ge h^{-1}$ for any trade-off functions g and h.

(b) If two trade-off functions f and g satisfy $f \geq g$, then $C_p(f) \geq C_p(g)$. This means that if a mechanism is more private than the other, using the same sampling ratio, the subsampled mechanism of the former remains more private than that of the latter, at least in terms of lower bounds.

(c) For any $0 \leq p \leq 1$, $C_p(\mathrm{Id}) = \mathrm{Id}$. That is, perfect privacy remains perfect privacy with subsampling.

Explicitly, we provide a formula to calculate $C_p(f)$ for a symmetric trade-off function f. Letting x^* be the unique fixed point of f, that is $f(x^*) = x^*$, we have

$$C_p(f)(x) = \begin{cases} f_p(x), & x \in [0, x^*] \\ x^* + f_p(x^*) - x, & x \in [x^*, f_p(x^*)] \\ f_p^{-1}(x), & x \in [f_p(x^*), 1]. \end{cases} \tag{13}$$

This expression is almost self-evident from the left panel of Figure 6. Nevertheless, a proof of this formula is given in Appendix E. This formula, together with Theorem 9, allows us to get a closed-form characterization of the privacy amplification for (ε, δ)-DP.

Corollary 3. *If M is (ε, δ)-DP on X^m, then the subsampled mechanism $M \circ \mathtt{Sample}_m$ is $C_p(f_{\varepsilon,\delta})$-DP on X^n, where*

$$C_p(f_{\varepsilon,\delta})(\alpha) = \max\left\{ f_{\varepsilon',\delta'}(\alpha), 1 - p\delta - p\frac{\mathrm{e}^{\varepsilon} - 1}{\mathrm{e}^{\varepsilon} + 1} - \alpha \right\}. \tag{14}$$

Above, $\varepsilon' = \log(1 - p + p\mathrm{e}^{\varepsilon}), \delta' = p\delta$, and $p = \frac{m}{n}$.

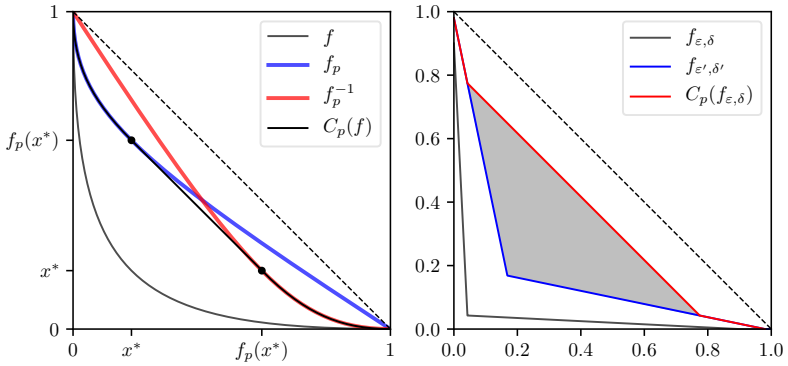

Fig. 6: The action of C_p. Left panel: $f = G_{1.8}, p = 0.35$. Right panel: $\varepsilon = 3, \delta = 0.1, p = 0.2$. The subsampling theorem 9 results in a significantly tighter trade-off function compared to the classical theorem for (ε, δ)-DP.

For comparison, we now present the existing bound on the privacy amplification by subsampling for (ε, δ)-DP. To be self-contained, Appendix E gives a proof of this result, which primarily follows Ullman (2017) .

lemma 2 (Ullman (2017))**.** *If M is (ε, δ)-DP, then $M \circ \mathtt{Sample}_m$ is (ε', δ')-DP with ε' and δ' defined in Corollary 3.*

Using the language of the f-DP framework, Lemma 2 states that $M \circ \texttt{Sample}_m$ is $f_{\varepsilon',\delta'}$-DP. Corollary 3 improves on Lemma 2 because, as is clear from (14), $C_p(f_{\varepsilon,\delta}) \geq f_{\varepsilon',\delta'}$. The right panel of Figure 6 illustrates Lemma 2 and our Corollary 3 for $\varepsilon = 3, \delta = 0.1$, and $p = 0.2$. In effect, the improvement is captured by the shaded triangle enclosed by $C_p(f_{\varepsilon,\delta})$ and $f_{\varepsilon',\delta'}$, revealing that the minimal sum of type I and type II errors in distinguishing two neighboring datasets with subsampling can be significantly lower than the prediction of Lemma 2. This gain is only made possible by the flexibility of trade-off functions in the sense that $C_p(f_{\varepsilon,\delta})$ *cannot* be expressed within the (ε, δ)-DP framework. The unavoidable loss in the (ε, δ)-DP representation of the subsampled mechanism is compounded when analyzing the composition of many private mechanisms.

In the next subsection, we prove Theorem 9 by making use of Lemma 2. Its proof implies that Theorem 9 holds for any subsampling scheme for which Lemma 2 is true. In particular, it holds for the subsampling scheme described at the beginning of this section, that is, independent coin flips for every data item.

4.2. Proof of the Subsampling Theorem

The proof strategy is as follows. First, we convert the f-DP guarantee into an infinite collection of (ε, δ)-DP guarantees by taking a dual perspective that is enabled by Proposition 6. Next, by applying the classical subsampling theorem (that is, Lemma 2) to these (ε, δ)-DP guarantees, we conclude that the subsampled mechanism satisfies a new infinite collection of (ε, δ)-DP guarantees. Finally, Proposition 5 allows us to convert these new privacy guarantees back into an $\tilde{f}$-DP guarantee, where $\tilde{f}$ can be shown to coincide with $C_p(f)$.

Proof of Theorem 9. Provided that M is f-DP, from Proposition 6 it follows that M is $\big(\varepsilon, \delta(\varepsilon)\big)$-DP with $\delta(\varepsilon) = 1 + f^*(-\mathrm{e}^{\varepsilon})$ for all $\varepsilon \geqslant 0$. Making use of Lemma 2, the subsampled mechanism $M \circ \texttt{Sample}_m$ satisfies the following collection of (ε', δ')-DP guarantees for all $\varepsilon \geqslant 0$:

$$\varepsilon' = \log(1 - p + p\mathrm{e}^{\varepsilon}), \quad \delta' = p\big(1 + f^*(-\mathrm{e}^{\varepsilon})\big).$$

Eliminating the variable ε from the two parametric equations above, we can relate ε' to δ' using

$$\delta' = 1 + f_p^*(-\mathrm{e}^{\varepsilon'}), \tag{15}$$

which is proved in Appendix E. The remainder of the proof is devoted to showing that (ε', δ')-DP guarantees for all $\varepsilon' \geq 0$ is equivalent to the $C_p(f)$-DP guarantee.

At first glance, (15) seems to enable the use of Proposition 6. Unfortunately, that would be invalid because f_p is asymmetric. To this end, we need to extend Proposition 6 to general trade-off functions. To avoid conflicting notation, let g be a generic trade-off function, not necessarily symmetric. Denote by $\bar{x}$ be the smallest point such that $g'(x) = -1$, that is, $\bar{x} = \inf\{x \in [0,1] : g'(x) = -1\}$. As a special instance of Proposition E.1 in the appendix, the following result serves our purpose.

Proposition 8. *If $g(\bar{x}) \geqslant \bar{x}$ and a mechanism M is $(\varepsilon, 1 + g^*(-\mathrm{e}^{\varepsilon}))$-DP for all $\varepsilon \geqslant 0$, then M is $\min\{g, g^{-1}\}^{**}$-DP.*

The proof of the present theorem would be complete if Proposition 8 can be applied to the collection of privacy guarantees in (15)for f_p. To use Proposition 8, it suffices to verify the condition $f_p(\bar{x}) \geqslant \bar{x}$ where $\bar{x}$ is the smallest point such that $f_p'(x) = -1$. Let x^* be the (unique) fixed point of f. To this end, we collect a few simple facts:

- First, $f'(x^*) = -1$. This is because the graph of f is symmetric with respect to the 45° line passing through the origin.
- Second, $\bar{x} \leqslant x^*$. This is because $f_p'(x^*) = pf'(x^*) + (1-p)\mathrm{Id}'(x^*) = -1$ and, by definition, $\bar{x}$ can only be smaller.

With these facts in place, we get

$$f_p(\bar{x}) \geqslant f_p(x^*) \geqslant f(x^*) = x^* \geqslant \bar{x}$$

by recognizing that f_p is decreasing and $f_p \geq f$. Hence, the proof is complete.

□

5. Application: Privacy Analysis of Stochastic Gradient Descent

One of the most important algorithms in machine learning and optimization is stochastic gradient descent (SGD). This is an iterative optimization method used to train a wide variety of models, for example, deep neural networks. SGD has also served as an important benchmark in the development of private optimization: as an iterative algorithm, the tightness of its privacy analysis crucially depends on the tightness with which composition can be accounted for. The analysis also crucially requires a privacy amplification by subsampling argument.

The first asymptotically optimal analysis of differentially private SGD was given by Bassily et al. (2014). Because of the inherent limits of (ε, δ)-DP, however, this analysis stops short of giving meaningful privacy bounds for realistically sized datasets. This is in part what motivated the development of divergence based relaxations of differential privacy. Unfortunately, these relaxations cannot be directly applied to the analysis of SGD due to the lack of a privacy amplification by subsampling theorem. In response, Abadi et al. (2016) circumvented this challenge by developing the moments accountant—a numeric technique tailored specifically to repeated application of subsampling, followed by a Gaussian mechanism—to give privacy bounds for SGD that are strong enough to give non-trivial guarantees when training deep neural networks on real datasets. But this analysis is ad-hoc in the sense that it uses a tool designed specifically for the analysis of SGD.

In this section, we use the general tools we have developed so far to give a simple and improved analysis of the privacy of SGD. In particular, the analysis rests crucially on the compositional and subsampling properties of f-DP.

5.1. Stochastic Gradient Descent and Its Privacy Analysis

Letting $S = (x_1, \ldots, x_n)$ denote the dataset, consider minimizing the empirical risk

$$\frac{1}{n}\sum_{i=1}^{n} L(\theta, x_i)$$

over the parameter θ, where $L(\theta, x_i)$ denotes a loss function. At iteration t, a set I_t of size m is selected uniformly at random from $\{1, 2, \ldots, n\}$. Taking learning rate η_t, SGD seeks to minimize the empirical risk by running

$$\theta_{t+1} = \theta_t - \eta_t \cdot \frac{1}{m} \sum_{i \in I_t} \nabla_\theta L(\theta_t, x_i)$$

from an initial point θ_0.

Algorithm 1 `NoisySGD`

1: **Input:** Dataset $S = (x_1, \ldots, x_n)$, loss function $L(\theta, x)$.
Parameters: initial state θ_0, learning rate η_t, batch size m, time horizon T, noise scale σ, gradient norm bound C.
2: **for** $t = 1, \ldots, T$ **do**
3: **Subsampling:**
Take a uniformly random subsample $I_t \subseteq \{1, \ldots, n\}$ of size m ▷ $\texttt{Sample}_m$ in Section 4
4: **for** $i \in I_t$ **do**
5: **Compute gradient:**
$v_t^{(i)} \leftarrow \nabla_\theta L(\theta_t, x_i)$
6: **Clip gradient:**
$\bar{v}_t^{(i)} \leftarrow v_t^{(i)} / \max\left\{1, \|v_t^{(i)}\|_2 / C\right\}$
7: **Average, perturb, and descend:**
$\theta_{t+1} \leftarrow \theta_t - \eta_t \Big(\frac{1}{m} \sum_{i \in I_t} \bar{v}_t^{(i)} + \mathcal{N}(0, \frac{4\sigma^2 C^2}{m^2} I) \Big)$ ▷ I is an identity matrix
8: **Output** θ_T

A private variant of this optimization algorithm is described in Algorithm 1. We refer to this private algorithm as `NoisySGD`, which can be viewed as a repeated composition of Gaussian mechanisms operating on subsampled datasets. To analyze the privacy of `NoisySGD`, we start by building up the privacy properties from the inner loop. Let V be the vector space where parameter θ lives in and $M : X^m \times V \to V$ be the mechanism that executes lines 4-7 in Algorithm 1. Here m denotes the batch size. In effect, what M does in iteration t can be expressed as

$$M(S_{I_t}, \theta_t) = \theta_{t+1},$$

where S_{I_t} is the subset of the dataset S indexed by I_t. Next, we turn to the analysis of the subsampling step (line 3) and use $\widetilde{M}$ to denote its composition with M, that is, $\widetilde{M} = M \circ \texttt{Sample}_m$. Taken together, $\widetilde{M}$ executes lines 3-7 and maps from $X^n \times V$ to V.

The mechanism we are ultimately interested in

$$\begin{aligned} \texttt{NoisySGD} : X^n &\to V \times V \times \cdots \times V \\ S &\mapsto (\theta_1, \theta_2, \ldots, \theta_T) \end{aligned}$$

is simply the composition of T copies of $\widetilde{M}$. To see this fact, note that the trajectory $(\theta_1, \theta_2, \ldots, \theta_T)$ is obtained by iteratively running

$$\theta_{j+1} = \widetilde{M}(S, \theta_j)$$

for $j = 0, \ldots, T-1$. Let M be f-DP. Straightforwardly, $\widetilde{M}$ is $C_{m/n}(f)$-DP by Theorem 9. Then, from the composition theorem (Theorem 4), we can readily prove that `NoisySGD` is $C_{m/n}(f)^{\otimes T}$-DP.

Hence, it suffices to give a bound on the privacy of M. For simplicity, we now focus on a single step and drop the subscript t. Recognizing that changing one of the m data points only affects one $v^{(i)}$, the sensitivity of $\frac{1}{m}\sum_i \bar{v}_t^{(i)}$ is at most $\frac{2C}{m}$ due to the clipping operation. Making use of Theorem 1, adding Gaussian noise $N(0, \sigma^2 \cdot \frac{4C^2}{m^2} I)$ to the average gradient renders this step $\frac{1}{\sigma}$-GDP. Since that the gradient update following the gradient averaging step is deterministic, we conclude that M satisfies $\frac{1}{\sigma}$-GDP.

In summary, the discussion above has proved the following theorem:

Theorem 10. *Algorithm 1 is $C_{m/n}(G_{\sigma^{-1}})^{\otimes T}$-DP.*

To clear up any confusion, we remark that this $C_{m/n}(G_{\sigma^{-1}})^{\otimes T}$-DP mechanism does not release the subsampled indices.

The use of Theorem 10 relies on an efficient evaluation of $C_{m/n}(G_{\sigma^{-1}})^{\otimes T}$. Our central limit theorems provide an analytical approach to approximating this tensor product and the approximation is accurate for large T. The next two subsections present two such results, corresponding to our two central limit theorems (Theorem 5 and Theorem 6), respectively. An asymptotic privacy analysis of `NoisySGD` is given in Section 5.2 by developing a general limit theorem for composition of subsampled mechanisms, and an illustration of this result is shown in Figure 7. A Berry–Esseen type analysis is developed in Section 5.3. The implementation of our privacy analysis of `NoisySGD` is available in the `TensorFlow privacy` package (`https://github.com/tensorflow/privacy`); see details in `https://github.com/tensorflow/privacy/blob/master/tensorflow_privacy/privacy/analysis/gdp_accountant.py`.

5.2. Asymptotic Privacy Analysis

In this subsection, we first consider the limit of $C_p(f)^{\otimes T}$ for a general trade-off function f, then plug in $f = G_{\sigma^{-1}}$ for the analysis of `NoisySGD`. The more general approach is useful for analyzing other iterative algorithms.

Recall from Section 4 that a p-subsampled f-DP mechanism is $C_p(f)$-DP, where $C_p(f)$ is defined as

$$C_p(f)(x) = \begin{cases} f_p(x), & x \in [0, x^*] \\ x^* + f_p(x^*) - x, & x \in [x^*, f_p(x^*)] \\ f_p^{-1}(x), & x \in [f_p(x^*), 1], \end{cases}$$

where x^* is the unique fixed point of f. We will let the sampling fraction p tend to 0 as T approaches infinity. In the following theorem, a_+^2 is a short-hand for $(\max\{a, 0\})^2$.

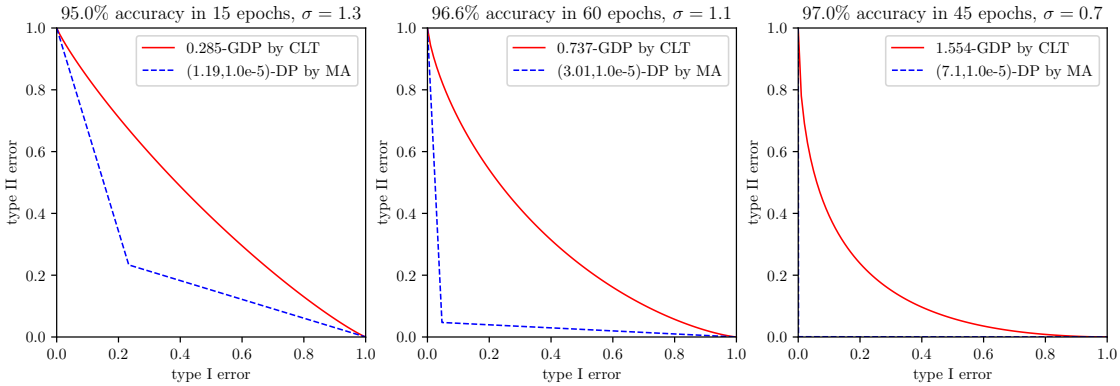

Fig. 7: Comparison of the GDP bounds derived from our method, and the (ε, δ)-DP bounds derived using the moments accountant (Abadi et al., 2016), which is essentially based on Rényi differential privacy (Mironov, 2017). All three experiments run Algorithm 1 on the entire MNIST dataset with $n = 60,000$ data points, batch size $m = 256$, learning rates η_t set to 0.25, 0.15, and 0.25, respectively, and clipping thresholds C set to 1.5, 1.0, 1.5, respectively. The red lines are obtained via Corollary 4, while the blue dashed lines are produced by the tensorflow/privacy library. See `https://github.com/tensorflow/privacy` for the details of the setting and more experiments in follow-up work (Bu et al., 2019).

Theorem 11. *Suppose f is a symmetric trade-off function such that $f(0) = 1$ and $\int_0^1 (f'(x)+1)^4 \, \mathrm{d}x < +\infty$. Furthermore, assume $p\sqrt{T} \to p_0$ as $T \to \infty$ for some constant $p_0 > 0$. Then we have the uniform convergence*

$$C_p(f)^{\otimes T} \to G_{p_0\sqrt{2\chi_+^2(f)}}$$

as $T \to \infty$, where

$$\chi_+^2(f) = \int_0^1 \left(|f'(x)| - 1\right)_+^2 \mathrm{d}x.$$

The proof is deferred to Appendix F. This theorem has implications for the design of iterative private mechanisms involving subsampling as a subroutine. One way to bound the privacy of such a mechanism is to let the sampling ratio p go to zero as the total number of iterations T goes to infinity. The theorem says that the correct scaling between the two values is $p \sim 1/\sqrt{T}$ and, furthermore, gives an explicit form of the limit.

In order to analyze `NoisySGD`, we need to compute the quantity $\chi_+^2(G_\mu)$. This can be done by directly working with its definition. In Appendix F, we provide a different approach by relating $\chi_+^2(f)$ to χ^2-divergence.

lemma 3. *We have*

$$\chi_+^2(G_\mu) = \mathrm{e}^{\mu^2} \cdot \Phi(3\mu/2) + 3\Phi(-\mu/2) - 2.$$

When using SGD to train large models, we typically perform a very large number of iterations, so it is reasonable to consider the parameter regime in which $n \to \infty, T \to \infty$.

The batch size can also vary with these quantities. The following result is a direct consequence of Theorems 10 and 11 and Lemma 3.

Corollary 4. *If $m\sqrt{T}/n \to c$ for a constant $c > 0$, then* `NoisySGD` *is asymptotically μ-GDP with*

$$\mu = \sqrt{2}c \cdot \sqrt{\mathrm{e}^{\sigma^{-2}} \cdot \Phi(1.5\sigma^{-1}) + 3\Phi(-0.5\sigma^{-1}) - 2}.$$

The condition required in this theorem is more general than that required in the analysis of private SGD by Bassily et al. (2014), which assumes $m = 1$ and $T = O(n^2)$. Moreover, we note that $\frac{m}{n} \cdot \sqrt{T}$ in deep learning research is generally quite small. The convention in this literature is to reparameterize the number of gradient steps T by the number of "epochs" E, which is the number of sweeps of the entire dataset. The relationship between these parameters is that $E = Tm/n$. In this reparameterization, our assumption is that $Em/n \to c^2$. Concretely, the AlexNet (Krizhevsky et al., 2012) sets the parameters as $m = 128, E \approx 90$ on the ILSVRC-2010 dataset with $n \approx 1.2 \times 10^6$, leading to $Em/n < 0.01$. Many other prominent implementations also lead to a small value of Em/n. See the webpage of the Gluon CV Toolkit (He et al., 2018; Zhang et al., 2019) for a collection of such hyperparameters in computer vision tasks.

5.3. A Berry–Esseen Privacy Bound

Now, we apply the Berry–Esseen style central limit theorem (Theorem 5) to the privacy analysis of `NoisySGD`, highlighting the advantage of giving sharp privacy guarantees. However, the shortcoming is that the expressions that it yields are more unwieldy: they are computer evaluable, so usable in implementations, but do not admit simple closed forms.

The individual components in Theorem 5 have the form $C_p(G_\mu)$ with $p = m/n, \mu = \sigma^{-1}$. It suffices to evaluate the moment functionals on $C_p(G_\mu)$. This is done in the following lemma, with its proof given in Appendix F.

lemma 4. *Let $Z(x) = \log(p \cdot \mathrm{e}^{\mu x - \mu^2/2} + 1 - p)$ and $\varphi(x) = \frac{1}{\sqrt{2\pi}}\mathrm{e}^{-x^2/2}$ be the density of the standard normal distribution. Then*

$$\begin{aligned}
\mathrm{kl}\big(C_p(G_\mu)\big) &= p \int_{\mu/2}^{+\infty} Z(x) \cdot \big(\varphi(x-\mu) - \varphi(x)\big)\,\mathrm{d}x \\
\kappa_2\big(C_p(G_\mu)\big) &= \int_{\mu/2}^{+\infty} Z^2(x) \cdot \big(p\varphi(x-\mu) + (2-p)\varphi(x)\big)\,\mathrm{d}x \\
\bar{\kappa}_3\big(C_p(G_\mu)\big) &= \int_{\mu/2}^{+\infty} \big|Z(x) - \mathrm{kl}\big(C_p(G_\mu)\big)\big|^3 \cdot (p\varphi(x-\mu) + (1-p)\varphi(x))\,\mathrm{d}x \\
&\quad + \int_{\mu/2}^{+\infty} \big|Z(x) + \mathrm{kl}\big(C_p(G_\mu)\big)\big|^3 \cdot \varphi(x)\,\mathrm{d}x.
\end{aligned}$$

By plugging these expressions into Theorem 5, we get

Corollary 5. *Let* $p = m/n, \mu = \sigma^{-1}$ *and*

$$\tilde{\mu} = \frac{2\sqrt{T} \cdot \mathrm{kl}\big(C_p(G_\mu)\big)}{\sqrt{\kappa_2\big(C_p(G_\mu)\big) - \mathrm{kl}^2\big(C_p(G_\mu)\big)}}, \quad \gamma = \frac{0.56}{\sqrt{T}} \cdot \frac{\bar{\kappa}_3\big(C_p(G_\mu)\big)}{\big(\kappa_2\big(C_p(G_\mu)\big) - \mathrm{kl}^2\big(C_p(G_\mu)\big)\big)^{\frac{3}{2}}}.$$

Then, `NoisySGD` *is* f*-DP with* $f(\alpha) = \max\{G_{\tilde{\mu}}(\alpha + \gamma) - \gamma, 0\}$.

We remark that $G_{\tilde{\mu}}$ can be set to 0 in $(1, +\infty)$ so that f is well-defined for $\alpha > 1 - \gamma$.

6. Discussion

In this paper, we have introduced a new framework for private data analysis that we refer to as f-differential privacy, which generalizes (ε, δ)-DP and has a number of attractive properties that escape the difficulties of prior work. This new privacy definition uses trade-off functions of hypothesis testing as a measure of indistinguishability of two neighboring datasets rather than a few parameters as in prior differential privacy relaxations. Our f-DP retains an interpretable hypothesis testing semantics and is expressive enough to losslessly reason about composition, post-processing, and group privacy by virtue of the informativeness of trade-off functions. Moreover, f-DP admits a central limit theorem that identifies a simple and single-parameter family of privacy definitions as focal: Gaussian differential privacy. Precisely, all hypothesis testing based definitions of privacy converge to Gaussian differential privacy in the limit under composition, which implies that Gaussian differential privacy is the unique such definition that can tightly handle composition. The central limit theorem and its Berry–Esseen variant give a tractable analytical approach to tightly analyzing the privacy cost of iterative methods such as SGD. Notably, f-DP is *dual* to (ε, δ)-DP in a constructive sense, which gives the ability to import results proven for (ε, δ)-DP. This powerful perspective allows us to obtain an easy-to-use privacy amplification by subsampling theorem for f-DP, which in particular significantly improves on the state-of-the-art counterpart in the (ε, δ)-DP setting.

We see several promising directions for future work using and extending the f-DP framework. First, Theorem 8 can possibly be extended to the inhomogeneous case where trade-off functions are different from each other in the composition. Such an extension would allow us to apply the central limit theorem for privacy approximation with strong finite-sample guarantees to a broader range of problems. Second, it would be of interest to investigate whether the privacy guarantee of the subsampled mechanism in Theorem 9 can be improved for some trade-off functions. Notably, we have shown in Appendix E that this bound is tight if the trade-off function $f = 0$, that is, the original mechanism is blatantly non-private. Third, the notion of f-DP naturally has a *local* realization where the obfuscation of the sensitive information is applied at the individual record level. In this setting, what are the fundamental limits of estimation with local f-DP guarantees (Duchi et al., 2018)? In light of Duchi and Ruan (2018), what is the correct complexity measure in local f-DP estimation? If it is not the Fisher information, can we identify an alternative to the Fisher information for some class of trade-off functions? Moreover, we recognize that an adversary in differentially private learning may set different pairs of target type I and type II errors. For example, an adversary that attempts to control type

I and II errors at 10% and 10%, respectively, can behave very differently from one who aims to control the two errors at 0.1% and 99%, respectively. An important question is to address the trade-offs between resources such as privacy and statistical efficiency and target type I and type II errors in the framework of f-DP.

Finally, we wish to remark that f-DP can possibly offer a mathematically tractable and flexible framework for minimax estimation under privacy constraints (see, for example, Cai et al. (2019); Bun et al. (2018b); Dwork et al. (2015)). Concretely, given a candidate estimator satisfying (ε, δ)-DP appearing in the upper bound and a possibly loose lower bound under the (ε, δ)-DP constraint, we can replace the (ε, δ)-DP constraint by the f-DP constraint where f is the tightest trade-off function characterizing the estimation procedure. As is clear, the f-DP constraint is more stringent than the (ε, δ)-DP constraint by recognizing the primal-dual conversion (see Proposition 6). While the upper bound remains the same as the estimator continues to satisfy the new privacy constraint, the lower bound can be possibly improved due to a more stringent constraint. It would be of great interest to investigate to what extent this f-DP based approach can reduce the gap between upper and lower bounds minimax estimation under privacy constraints.

Ultimately, the test of a privacy definition lies not just in its power and semantics, but also in its ability to usefully analyze diverse algorithms. In this paper, we have given convincing evidence that f-DP is up to the task. We leave the practical evaluation of this new privacy definition to future work.

7. Supplemental Materials

Due to space constraints, we have relegated proofs of theorems and other technical details to the on-line appendices appendix A–appendix F in the Supplement to "Gaussian Differential Privacy." Python code for analyzing the privacy loss of SGD in the f-DP framework is available at `https://github.com/tensorflow/privacy/blob/master/tensorflow_privacy/privacy/analysis/gdp_accountant.py`.

Acknowledgements

We would like to thank the associate editor and the referees for constructive comments that improved the presentation of the paper. This work was supported in part by NSF grants CAREER DMS-1847415, CCF-1763314, and CNS-1253345, by the Sloan Foundation, and by a sub-contract for the DARPA Brandeis program.

References

M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang. Deep learning with differential privacy. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 308–318. ACM, 2016.

J. M. Abowd. The US Census Bureau adopts differential privacy. In *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, pages 2867–2867. ACM, 2018.

D. P. T. Apple. Learning with privacy at scale. Technical report, Apple, 2017.

S. Arora and B. Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009.

B. Balle and Y.-X. Wang. Improving the Gaussian mechanism for differential privacy: Analytical calibration and optimal denoising. *arXiv preprint arXiv:1805.06530*, 2018.

B. Balle, G. Barthe, and M. Gaboardi. Privacy amplification by subsampling: Tight analyses via couplings and divergences. In *Advances in Neural Information Processing Systems*, pages 6280–6290, 2018.

M. Barbaro and T. Zeller. A face is exposed for AOL searcher no. 4417749. *The New York Times*, Aug. 2006. `http://select.nytimes.com/gst/abstract.html?res=F10612FC345B0C7A8CDDA10894DE404482`.

R. Bassily, A. Smith, and A. Thakurta. Private empirical risk minimization: Efficient algorithms and tight error bounds. In *2014 IEEE 55th Annual Symposium on Foundations of Computer Science*, pages 464–473. IEEE, 2014.

D. Blackwell. Comparison of experiments. Technical report, HOWARD UNIVERSITY Washington United States, 1950.

Z. Bu, J. Dong, Q. Long, and W. J. Su. Deep learning with Gaussian differential privacy. *arXiv preprint arXiv:1911.11607*, 2019.

M. Bun and T. Steinke. Concentrated differential privacy: Simplifications, extensions, and lower bounds. In *Theory of Cryptography Conference*, pages 635–658. Springer, 2016.

M. Bun, C. Dwork, G. N. Rothblum, and T. Steinke. Composable and versatile privacy via truncated cdp. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, pages 74–86. ACM, 2018a.

M. Bun, J. Ullman, and S. Vadhan. Fingerprinting codes and the price of approximate differential privacy. *SIAM Journal on Computing*, 47(5):1888–1938, 2018b.

T. T. Cai, Y. Wang, and L. Zhang. The cost of privacy: Optimal rates of convergence for parameter estimation with differential privacy. *arXiv preprint arXiv:1902.04495*, 2019.

B. Ding, J. Kulkarni, and S. Yekhanin. Collecting telemetry data privately. In *Proceedings of Advances in Neural Information Processing Systems 30 (NIPS 2017)*, 2017.

J. C. Duchi and F. Ruan. The right complexity measure in locally private estimation: It is not the fisher information. *arXiv preprint arXiv:1806.05756*, 2018.

J. C. Duchi, M. I. Jordan, and M. J. Wainwright. Minimax optimal procedures for locally private estimation. *Journal of the American Statistical Association*, 113(521): 182–201, 2018.

C. Dwork and G. N. Rothblum. Concentrated differential privacy. *arXiv preprint arXiv:1603.01887*, 2016.

C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor. Our data, ourselves: Privacy via distributed noise generation. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 486–503. Springer, 2006a.

C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of cryptography conference*, pages 265–284. Springer, 2006b.

C. Dwork, G. N. Rothblum, and S. Vadhan. Boosting and differential privacy. In *Foundations of Computer Science (FOCS), 2010 51st Annual IEEE Symposium on*, pages 51–60. IEEE, 2010.

C. Dwork, A. Smith, T. Steinke, J. Ullman, and S. Vadhan. Robust traceability from trace amounts. In *2015 IEEE 56th Annual Symposium on Foundations of Computer Science*, pages 650–669. IEEE, 2015.

Ú. Erlingsson, V. Pihur, and A. Korolova. Rappor: Randomized aggregatable privacy-preserving ordinal response. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, pages 1054–1067. ACM, 2014.

T. He, Z. Zhang, H. Zhang, Z. Zhang, J. Xie, and M. Li. Bag of tricks for image classification with convolutional neural networks. *arXiv preprint arXiv:1812.01187*, 2018.

S. Holmes. Challenges in the analyses of multidomain longitudinal data: Layered solutions, 2019. 3rd Workshop on Statistical and Algorithmic Challenges in Microbiome Data Analysis.

N. Homer, S. Szelinger, M. Redman, D. Duggan, W. Tembe, J. Muehling, J. Pearson, D. Stephan, S. Nelson, and D. Craig. Resolving individuals contributing trace amounts of dna to highly complex mixtures using high-density snp genotyping microarrays. *PLoS Genetics*, 4(8):e1000167, 2008.

P. Kairouz, S. Oh, and P. Viswanath. The composition theorem for differential privacy. *IEEE Transactions on Information Theory*, 63(6):4037–4049, 2017.

S. P. Kasiviswanathan, H. K. Lee, K. Nissim, S. Raskhodnikova, and A. Smith. What can we learn privately? *SIAM Journal on Computing*, 40(3):793–826, 2011.

A. Krizhevsky, I. Sutskever, and G. E. Hinton. Imagenet classification with deep convolutional neural networks. In *Advances in neural information processing systems*, pages 1097–1105, 2012.

Y. LeCun and C. Cortes. MNIST handwritten digit database. 2010. URL `http://yann.lecun.com/exdb/mnist/`.

I. Mironov. Rényi differential privacy. In *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*, pages 263–275. IEEE, 2017.

J. Murtagh and S. Vadhan. The complexity of computing the optimal composition of differential privacy. In *Theory of Cryptography Conference*, pages 157–175. Springer, 2016.

A. Narayanan and V. Shmatikov. Robust de-anonymization of large sparse datasets. In *2008 ieee symposium on security and privacy*, pages 111–125. IEEE, 2008.

M. Raginsky. Shannon meets blackwell and le cam: Channels, codes, and statistical experiments. In *2011 IEEE International Symposium on Information Theory Proceedings*, pages 1220–1224. IEEE, 2011.

D. Sommer, S. Meiser, and E. Mohammadi. Privacy loss classes: The central limit theorem in differential privacy. 2018.

J. Ullman. Cs7880: Rigorous approaches to data privacy, spring 2017. 2017. `http://www.ccs.neu.edu/home/jullman/PrivacyS17/HW1sol.pdf`.

V. V. Vazirani. *Approximation algorithms*. Springer Science & Business Media, 2013.

Y.-X. Wang, B. Balle, and S. Kasiviswanathan. Subsampled Rényi differential privacy and analytical moments accountant. *arXiv preprint arXiv:1808.00087*, 2018.

L. Wasserman and S. Zhou. A statistical framework for differential privacy. *Journal of the American Statistical Association*, 105(489):375–389, 2010.

Z. Zhang, T. He, H. Zhang, Z. Zhang, J. Xie, and M. Li. Bag of freebies for training object detection neural networks. *arXiv preprint arXiv:1902.04103*, 2019.

Q. Zheng, J. Dong, Q. Long, and W. J. Su. Sharp composition bounds for Gaussian differential privacy via Edgeworth expansion. *arXiv preprint arXiv:2003.04493*, 2020.