



Review

# GDP vs. LDP: A Survey from the Perspective of Information-Theoretic Channel

Hai Liu <sup>1,2,3</sup> , Changgen Peng <sup>1,2,3,\*</sup> , Youliang Tian <sup>2,3</sup>, Shigong Long <sup>2,3</sup>, Feng Tian <sup>4</sup> and Zhenqiang Wu <sup>4</sup>

<sup>1</sup> Guizhou Big Data Academy, Guizhou University, Guiyang 550025, China; liuhai@snnu.edu.cn

<sup>2</sup> College of Computer Science and Technology, Guizhou University, Guiyang 550025, China; yltian@gzu.edu.cn (Y.T.); sglong@gzu.edu.cn (S.L.)

<sup>3</sup> State Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025, China

<sup>4</sup> School of Computer Science, Shaanxi Normal University, Xi'an 710119, China; tianfeng@snnu.edu.cn (F.T.); zqiangwu@snnu.edu.cn (Z.W.)

\* Correspondence: cgpeng@gzu.edu.cn

**Abstract:** The existing work has conducted in-depth research and analysis on global differential privacy (GDP) and local differential privacy (LDP) based on information theory. However, the data privacy preserving community does not systematically review and analyze GDP and LDP based on the information-theoretic channel model. To this end, we systematically reviewed GDP and LDP from the perspective of the information-theoretic channel in this survey. First, we presented the privacy threat model under information-theoretic channel. Second, we described and compared the information-theoretic channel models of GDP and LDP. Third, we summarized and analyzed definitions, privacy-utility metrics, properties, and mechanisms of GDP and LDP under their channel models. Finally, we discussed the open problems of GDP and LDP based on different types of information-theoretic channel models according to the above systematic review. Our main contribution provides a systematic survey of channel models, definitions, privacy-utility metrics, properties, and mechanisms for GDP and LDP from the perspective of information-theoretic channel and surveys the differential privacy synthetic data generation application using generative adversarial network and federated learning, respectively. Our work is helpful for systematically understanding the privacy threat model, definitions, privacy-utility metrics, properties, and mechanisms of GDP and LDP from the perspective of information-theoretic channel and promotes in-depth research and analysis of GDP and LDP based on different types of information-theoretic channel models.

**Keywords:** GDP vs. LDP; information-theoretic channel; Rényi divergence; mutual information; expected distortion



**Citation:** Liu, H.; Peng, C.; Tian, Y.; Long, S.; Tian, F.; Wu, Z. GDP vs. LDP: A Survey from the Perspective of Information-Theoretic Channel. *Entropy* **2022**, *24*, 430. <https://doi.org/10.3390/e24030430>

Academic Editor: Boris Ryabko

Received: 6 February 2022

Accepted: 17 March 2022

Published: 19 March 2022

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

It is assumed that an attacker has background knowledge of name information about  $n$  patients in a medical dataset with a certain disease. The attacker can statistically query the sum of disease status of  $n - 1$  patients except the  $i$ -th patient and the sum of disease status with all  $n$  patients and then can infer whether the  $i$ -th patient has a disease by comparing the two statistical query results. To mitigate the problem of individual privacy leakage caused by the above statistical inference attack, Dwork et al. [1] proposed differential privacy (DP) to protect individual privacy independent of the presence or absence of any individual. Since DP requires that the data collector is trustworthy in a centralized setting, it is called centralized DP. Moreover, because DP considers global sensitivity of adjacent datasets, it is also known as global differential privacy (GDP). However, the data collector is untrusted in real-world applications. Therefore, Kasiviswanathan et al. [2] proposed that local differential privacy (LDP) allows an untrusted third party to perform statistical analysis while achieving user's privacy by random perturbation of local data. Both GDP and LDP have privacy-utility monotonicity and can achieve privacy-utility tradeoff [3].

GDP and LDP have become popular methods of data privacy preserving of the centralized and local setting, respectively. However, GDP and LDP have different advantages and disadvantages. In Table 1, we agree with Dobrota's [4] comparative analysis results of the advantages and disadvantages of GDP and LDP.

**Table 1.** Advantages and disadvantages of GDP and LDP.

Privacy Type	Advantage	Disadvantage
GDP	Better data utility	Needing trusted data collector
	Suitable for dataset of any scale	
LDP	Without needing trusted data collector	Poor data utility
		Not applicable to small scale dataset

Because of the advantages of using GDP and LDP in the centralized and local setting, respectively, the data privacy community has widely studied GDP and LDP based on information theory. The current work focuses on GDP and LDP from the following aspects based on information theory, including privacy threat model, channel models and definitions of GDP and LDP, privacy-utility metrics of GDP and LDP, properties of GDP and LDP, and mechanisms satisfying GDP and LDP. Unless otherwise stated, the information-theoretic channel model refers to the discrete single symbol information-theoretic channel in this survey. However, there is no review work to systematically survey the above existing work on GDP and LDP from the perspective of information-theoretic channel.

Therefore, this paper systematically surveyed GDP and LDP under the information-theoretic channel model from the aspects of resisting privacy threat model, channel models, definitions, privacy-utility metrics, properties, and achieving mechanisms. Our main contributions are as follows.

(1) We summarized the privacy threat model under information-theoretic channel, and we provided a systematic survey on channel models, definitions, privacy-utility metrics, properties, and mechanisms of GDP and LDP from the perspective of information-theoretic channel.

(2) We presented a comparative analysis between GDP and LDP from the perspective of information-theoretic channel. Then, we concluded the common channel models, definitions, privacy-utility metrics, properties, and achieving mechanisms of GDP and LDP in the existing work.

(3) We surveyed applications of GDP and LDP in synthetic data generation. Specifically, we first presented the membership inference attack and model extraction attack against generative adversarial network (GAN). Then, we reviewed the differential privacy synthetic data generation with GAN and differential privacy synthetic data generation with federated learning, respectively.

(4) Through analyzing the advantages and disadvantages of the existing work for different application scenarios and data types, we also discussed the open problems of GDP and LDP based on different types of information-theoretic channel models in the future.

This paper is organized as follows. Section 2 introduces the preliminaries. Section 3 summarizes the privacy threat model of centralized and local data setting under information-theoretic channel. Section 4 describes the channel models of GDP and LDP and uniformly states and analyzes the definitions of GDP and LDP under their channel models. Section 5 summarizes and compares the information-theoretic privacy-utility metrics of GDP and LDP. In Section 6, we present and analyze the properties of GDP and LDP from the perspective of information-theoretic channel. Section 7 summarizes and analyzes the mechanisms of GDP and LDP from the perspective of information-theoretic channel. Section 8 discusses the open problems of GDP and LDP from the perspective of different types of information-theoretic channel on different application scenarios and data types. Section 9 concludes this paper.

## 2. Preliminaries

In this section, we introduce the preliminaries of GDP [1], LDP [5], and the information-theoretic channel model and metrics [5–11]. The commonly used mathematical symbols are summarized in Table 2.

**Table 2.** Common mathematical symbols.

Symbol	Description
$x$	Dataset
$\mathcal{M}$	Randomized mechanism
$\varepsilon$	Privacy budget
$\delta$	Probability without satisfying differential privacy
$X$	Input random variable of information-theoretic channel
$Y$	Output random variable of information-theoretic channel
$p(y x)$	Channel transition probability matrix
$p(x)$	Probability distribution on source $X$
$q(x)$	Another probability distribution on source $X$
$D_\alpha(p(x)  q(x))$	Rényi divergence
$H_\alpha(X)$	Rényi entropy
$H(X)$	Shannon entropy
$H_\infty(X)$	Min-entropy
$H_\alpha(X Y)$	Conditional Rényi entropy
$H(X Y)$	Conditional Shannon entropy
$H_\infty(X Y)$	Conditional min-entropy
$I(X; Y)$	Mutual information
$I_\infty(X; Y)$	Max-information
$I_\infty^\beta(X; Y)$	$\beta$ -approximate max-information
$D_{\text{KL}}(p(x)  q(x))$	Kullback–Leibler divergence
$\Delta_f(p(x), q(x))$	$f$ -divergence
$\ p(x) - q(x)\ _{TV}$	Total variation distance
$D_\infty(p(x)  q(x))$	Max-divergence
$D_\infty^\delta(p(x)  q(x))$	$\delta$ -approximate max-divergence
$\bar{D}$	Expected distortion
$d(x_i, y_j)$	Single symbol distortion
$p_E$	Error probability
$\mathcal{H}$	A class of functions
$\Gamma$	A divergence
$D_\Gamma^{\mathcal{H}}(p(x), q(x))$	$\mathcal{H}$ -restricted $\Gamma$ -divergence
$D_f^{\mathcal{H}}(p(x), q(x))$	$\mathcal{H}$ -restricted $f$ -divergence
$D_{R,\alpha}^{\mathcal{H}}(p(x), q(x))$	$\mathcal{H}$ -restricted Rényi divergence

### 2.1. GDP and LDP

A dataset  $x$  is collections of records coming from a universal set  $X$ , and each  $x_i$  denotes the  $i$ -th item or a subset in the dataset  $x$ . When two datasets are different in only one item, the two datasets are adjacent datasets.

**Definition 1 (GDP).** A randomized mechanism  $\mathcal{M}$  with domain  $X$  is  $(\epsilon, \delta)$ -DP if for all  $S \subseteq \text{Range}(\mathcal{M})$  and for any two adjacent datasets  $x, x' \in X$ , it holds

$$p(\mathcal{M}(x) \in S) \leq e^\epsilon p(\mathcal{M}(x') \in S) + \delta \tag{1}$$

where the probability space is over the coin flips of the mechanism  $\mathcal{M}$ . If  $\delta = 0$ , then  $\mathcal{M}$  is  $\epsilon$ -DP.

The coin flips of the mechanism  $\mathcal{M}$  mean that a DP mechanism  $\mathcal{M}$  inherently has only equally likely outcomes with regard to each record of each individual. The equally likely to occur means that the probability distribution of response to any query is the same independent of any individual opting presence or absence in the dataset. If  $\mathcal{M}$  is  $(\epsilon, \delta)$ -DP, then  $\mathcal{M}$  is  $\epsilon$ -DP with probability at least  $1 - \delta$  for all datasets  $x$  and  $x'$  when  $x$  and  $x'$  are adjacent datasets. For the definition of LDP, the coin flips of mechanism  $\mathcal{M}$  have the same meanings.

**Definition 2 (LDP).** A randomized mechanism  $\mathcal{M}$  satisfies  $\epsilon$ -LDP if and only if for any pairs input values  $x$  and  $x'$  in the domain of  $X$ , and for any possible output  $z \in \text{Range}(\mathcal{M})$ , it holds

$$p(\mathcal{M}(z|x)) \leq e^\epsilon p(\mathcal{M}(z|x')) + \delta \tag{2}$$

where the probability space is over the coin flips of the mechanism  $\mathcal{M}$ . If  $\delta = 0$ , then  $\mathcal{M}$  is  $\epsilon$ -LDP.

### 2.2. Information-Theoretic Channel and Metrics

The mathematical model of an information-theoretic channel can be denoted by  $(X, p(y|x), Y)$ , where

- (1)  $X$  is an input random variable, and its value set is  $x = \{x_1, x_2, \dots, x_n\}$ .
- (2)  $Y$  is an output random variable, and its value set is  $y = \{y_1, y_2, \dots, y_m\}$ .
- (3)  $p(y|x)$  is the channel transition probability matrix, and the sum of the probabilities in each row satisfies  $\sum_{j=1}^m p(y_j|x_i) = 1$ .

In information-theoretic channel model, the Rényi divergence of a probability distribution  $p(x) = (p(x_1), p(x_2), \dots, p(x_n))$  on source  $X$  from another distribution  $q(x) = (q(x_1), q(x_2), \dots, q(x_n))$  is  $D_\alpha(p(x)||q(x)) = \frac{1}{\alpha-1} \log_2 \sum_{i=1}^n (p(x_i))^\alpha (q(x_i))^{1-\alpha}$ , where  $\alpha > 0$  and  $\alpha \neq 1$ . When  $q(x)$  is the uniform distribution with  $q(x) = (\frac{1}{n}, \dots, \frac{1}{n})$ , the Rényi entropy is  $H_\alpha(X) = \frac{1}{1-\alpha} \log_2 (\sum_{i=1}^n p(x_i)^\alpha)$  in terms of the Rényi divergence of  $p(x)$ . When  $\alpha \rightarrow 1$ , the Rényi entropy tends to the Shannon entropy  $H(X) = \lim_{\alpha \rightarrow 1} H_\alpha(X) = -\sum_{i=1}^n p(x_i) \log_2 p(x_i)$  of source  $X$ . When  $\alpha \rightarrow \infty$ , the Rényi entropy tends to the min-entropy  $H_\infty(X) = \lim_{\alpha \rightarrow \infty} H_\alpha(X) = -\log_2 \max_{x_i \in X} p(x_i)$ . The conditional Rényi entropy of  $X$  given  $Y$  is  $H_\alpha(X|Y) = -\log_2 (\sum_{j=1}^m p(y_j) (\sum_{i=1}^n (p(x_i|y_j))^\alpha)^{\frac{1}{\alpha}})^{\frac{\alpha}{\alpha-1}}$ . When  $\alpha \rightarrow 1$ , the conditional Rényi entropy is conditional Shannon entropy  $H(X|Y) = \lim_{\alpha \rightarrow 1} H_\alpha(X|Y) = \sum_{i=1}^n \sum_{j=1}^m p(x_i y_j) \log_2 p(x_i|y_j)$ . When  $\alpha \rightarrow \infty$ , the conditional Rényi entropy is conditional min-entropy  $H_\infty(X|Y) = \lim_{\alpha \rightarrow \infty} H_\alpha(X|Y) = -\log_2 \sum_{j=1}^m p(y_j) \max_{x_i \in X} p(x_i|y_j)$ . The mutual information  $I(X;Y) = H(X) - H(X|Y)$  is the average information measure of  $X$  contained in random variable  $Y$ . Furthermore, the max-information is  $I_\infty(X;Y) = H_\infty(X) - H_\infty(X|Y) = \max \log_2 \frac{p(x_i y_j)}{p(x_i) p(y_j)}$ , and the  $\beta$ -approximate max-information is  $I_\infty^\beta(X;Y) = \max \log_2 \frac{p(x_i y_j) - \beta}{p(x_i) p(y_j)}$ .

Moreover, when  $\alpha \rightarrow 1$ , the Rényi divergence is Kullback–Leibler (KL) divergence  $D_{\text{KL}}(p(x)||q(x)) = \lim_{\alpha \rightarrow 1} D_\alpha(p(x)||q(x)) = \sum_{i=1}^n p(x_i) \log_2 \frac{p(x_i)}{q(x_i)}$ . The KL-divergence is an instance of the family of  $f$ -divergence  $\Delta_f(p(x), q(x)) = \sum_{i=1}^n q(x_i) f(\frac{p(x_i)}{q(x_i)})$  with non-negative convex functions  $f(t) = t \ln t - t + 1$ . The total variation distance is also an instance of the family of  $f$ -divergence with  $f(t) = \frac{1}{2}|t - 1|$ , and the total variation distance between distributions  $p(x)$  and  $q(x)$  is  $\|p(x) - q(x)\|_{TV} = \frac{1}{2} \|p(x) - q(x)\|_1$ . When  $\alpha \rightarrow \infty$ ,

the Rényi divergence is is max-divergence  $D_\infty(p(x)||q(x)) = \max_{x_i \in X} \log_2 \frac{p(x_i)}{q(x_i)}$ , and the  $\delta$ -approximate max-divergence is  $D_\infty^\delta(p(x)||q(x)) = \max_{x_i \in X} \log_2 \frac{p(x_i) - \delta}{q(x_i)}$ .

The expected distortion between input random variable  $X$  and output random variable  $Y$  is

$$\bar{D} = \sum_{i=1}^n \sum_{j=1}^m p(x_i y_j) d(x_i, y_j) = \sum_{i=1}^n \sum_{j=1}^m p(x_i) p(y_j | x_i) d(x_i, y_j) \tag{3}$$

where the distance measurement  $d(x_i, y_j)$  is single symbol distortion. The average error probability is

$$p_E = \sum_{i=1}^n p(x_i) \sum_{j=1}^m p(y_j \neq x_i | x_i) \tag{4}$$

Thus, the average error probability is expected Hamming distortion, when  $d(x_i, y_j)$  is Hamming distortion in Equation (3).

### 3. Privacy Threat Model on Information-Theoretic Channel

To mitigate the statistical inference attack, the GDP has a strong adversary assumption in which an adversary knows  $n - 1$  dataset records and tries to identify the remaining one [12,13]. However, the adversary is usually computationally bounded. Thus, Mironov [11] and Mir [14] assumed that the adversary has prior knowledge over the set of possible input dataset  $X$ . Furthermore, Smith [15] proposed one-try attack, where an adversary is allowed to ask exactly one question about form, “is  $X = x_i$ ?”. The Rényi min-entropy of  $X$  denotes the probability of success for one-try attack with the best strategy, which chooses the  $x_i$  with maximum probability. The conditional Rényi min-entropy of  $X$  given  $Y$  captures the probability of guessing the value of  $X$  in one single try when the output of  $Y$  is known. Therefore, the privacy leakage of channel model is Rényi min-entropy leakage  $I_\infty(X; Y) = H_\infty(X) - H_\infty(X|Y)$  under one-try attack [7]. The Rényi min-entropy leakage is max-information, and it is the ratio of the probabilities of attack success with a priori probability and a posterior probability. Thus, a Rényi min-entropy leakage corresponds to the concept of Bayes risk, which can also be regarded as a measure of the effectiveness of the attack. The maximal leakage  $\max_{p(x)} I_\infty(X; Y)$  is the maximal reduction in uncertainty about  $X$  when  $Y$  is observed [16]. The maximal leakage is taken by maximizing over all input distributions.

When adversary possesses knowledge of a priori probability distribution of input, LDP can lead to the risk of privacy leakage [2,17–22]. However, a better privacy-utility tradeoff can be achieved by incorporating the attacker’s knowledge into the LDP. Therefore, data utility can be improved by explicitly modeling the adversary’s prior knowledge of the LDP.

To sum up, the privacy threat of information-theoretic channel refers to the Bayes risk on input  $X$ , when attack known output  $Y$ . Thus, GDP and LDP can be used to mitigate the above privacy threat on information-theoretic channel for numerical data and categorical data, respectively.

### 4. Information-Theoretic Channel Models and Definitions of GDP and LDP

In this section, we summarize and compare information-theoretic channel models of GDP and LDP. Furthermore, we present the information-theoretic definitions of GDP and LDP under their information-theoretic channel models and compare the definitions of GDP (LDP) with other information-theoretic privacy definitions.

#### 4.1. Information-Theoretic Channel Models of GDP and LDP

In Table 3, Alvim et al. [7] had constructed an information-theoretic channel model  $(X, P(z|x), Z)$  of GDP to any query function  $f : X \rightarrow Y$  of adjacent datasets, where  $P(z|x)$  is DP mapping on input dataset  $X$  and random output  $Z$  of real output  $Y$ . Similarly, we can also construct an information-theoretic channel model  $(X, p(z|x), Z)$  of LDP to any different single input  $x$  and  $x'$ , where  $p(z|x)$  is LDP mapping on categorical dataset

$x = \{0, 1, \dots, n - 1\}$  of single input and categorical dataset  $z = \{0, 1, \dots, n - 1\}$  of single random output. Next, we will survey and compare the information-theoretic definitions of GDP and LDP under the above given information-theoretic channel models.

**Table 3.** Information-theoretic channel models of GDP and LDP.

Privacy Type	Data Type	Input	GDP and LDP Mapping	Real Output	Random Output	Adjacent Relationship
GDP [7]	Numerical data	Dataset	$X \{p(z x) : p(z x) \leq e^\epsilon p(z x')\}$	$Y$	$Z$	$x$ and $x'$ are adjacent datasets.
LDP	Categorical data	Data item	$X \{p(z x) : p(z x) \leq e^\epsilon p(z x')\}$	$X$	$Z$	$x$ and $x'$ are different.

4.2. Information-Theoretic Definitions of GDP and LDP

In Table 4, we summarize the current work on definitions of GDP using different information-theoretic metrics under the information-theoretic channel model. Alvim et al. [7] intuitively gave the definition of  $\epsilon$ -DP using transition probability distribution  $p(z|x)$  for all  $z \in Z, x, x' \in X$  with adjacent datasets  $x$  and  $x'$ . Barthe and Olmedo [8] defined  $(\epsilon, \delta)$ -DP based on  $f$ -divergence, which is a redefinition of DP. Dwork and Roth [9] gave the definitions of  $\epsilon$ -DP and  $(\epsilon, \delta)$ -DP based on max-divergence, which is an equivalent definition of DP from the perspective of information-theoretic channel. Mironov [11] defined the  $(\alpha, \epsilon)$ -Rényi DP (RDP) using Rényi divergence, and  $(\alpha, \epsilon)$ -RDP satisfies  $(\epsilon + \frac{\log \frac{1}{\alpha}}{\alpha - 1}, \delta)$ -DP. When  $\alpha \rightarrow \infty$ ,  $(\alpha, \epsilon)$ -RDP is  $\epsilon$ -DP according to the max-divergence. Conversely,  $\epsilon$ -DP is  $(\alpha, \frac{1}{2}\epsilon^2\alpha)$ -RDP [23]. We can conclude that RDP is a generalization of GDP. When  $\alpha \rightarrow 1$ ,  $(1, \epsilon)$ -RDP is the definitions of  $(\epsilon, \delta)$ -DP based on the KL-divergence of Reference [8]. When  $\alpha \rightarrow \infty$ ,  $(\infty, \epsilon)$ -RDP is the definitions of  $\epsilon$ -DP and  $(\epsilon, \delta)$ -DP based on the maximum divergence of Reference [9]. According to the  $f$ -divergence, Asoodeh et al. [24] also established the optimal relationship between RDP and  $(\epsilon, \delta)$ -DP to help to derive the optimal  $(\epsilon, \delta)$ -DP parameters of a mechanism for a given level of RDP. Chaudhuri et al. [25] defined  $(\mathcal{H}, \Gamma)$ -capacity bounded DP based on  $\mathcal{H}$ -restricted divergence, where  $\mathcal{H}$  is a class of functions and  $\Gamma$  is a divergence. The  $(\mathcal{H}, \Gamma)$ -capacity bounded DP relaxes GDP by restricting the adversary to attack or post-process the output of a privacy mechanism using functions drawn from a restricted function class  $\mathcal{H}$  and models adversaries of this form with restricted  $f$ -divergences between probability distributions on datasets different from a single record. The  $\mathcal{H}$ -restricted  $f$ -divergence is  $D_f^{\mathcal{H}}(p(x), q(x)) = \sup_{h \in \mathcal{H}} \mathbb{E}_{x \sim p(x)}[h(x)] - \mathbb{E}_{x \sim q(x)}[f^*(h(x))]$ , where  $f^*$  is Fenchel conjugate and  $f^*(s) = \sup_{x \in \mathbb{R}} x \cdot (s - f(x))$ . The  $\mathcal{H}$ -restricted Rényi divergence is  $D_{R,\alpha}^{\mathcal{H}}(p(x), q(x)) = \frac{\log(1 + \alpha(\alpha - 1)D_{R,\alpha}^{\mathcal{H}}(p(x), q(x)))}{\alpha - 1}$ , where  $D_{R,\alpha}^{\mathcal{H}}$  is the  $\mathcal{H}$ -restricted Rényi divergence of order  $\alpha$ . When  $\mathcal{H}$  is the class of all functions and  $\Gamma$  is the Rényi divergence, this definition reduced to RDP. Additionally, when  $\Gamma$  is the  $f$ -divergence, this definition is  $(\epsilon, \delta)$ -DP of Reference [8]. Thus, capacity bounded DP is a generalization of RDP.

**Table 4.** GDP definitions using different information-theoretic metrics.

Existing Work	Privacy Type	Information-Theoretic Metric	Formula	Description
DP [7]	$\epsilon$ -DP	Channel transition probability	$p(z x) \leq e^\epsilon p(z x')$	The transition probability matrix is used as the GDP mapping.
DP [8]	$(\epsilon, \delta)$ -DP	$f$ -divergence	$\Delta_{e^\epsilon} = \max d_{e^\epsilon}(p(z x), p(z x'))$ $d_{e^\epsilon} = \max\{p(z x) - e^\epsilon p(z x'), p(z x') - e^\epsilon p(z x), 0\}$ $\Delta_{e^\epsilon}(p(z x), p(z x')) \leq \delta$	$f$ -divergence includes KL-divergence.
DP [9]	$\epsilon$ -DP	Max-divergence	$D_\infty(p(z x)  p(z x')) \leq \epsilon$ $D_\infty(p(z x')  p(z x)) \leq \epsilon$	Since the max-divergence is not symmetric and does not satisfy triangular inequality, the reciprocal of equation must be true.
	$(\epsilon, \delta)$ -DP		$D_\infty^\delta(p(z x)  p(z x')) \leq \epsilon$ $D_\infty^\delta(p(z x')  p(z x)) \leq \epsilon$	
$(\alpha, \epsilon)$ -RDP [11]	$\epsilon$ -DP	Rényi divergence	$D_\alpha(p(z x)  p(z x')) \leq \epsilon$	When $\alpha \rightarrow \infty$ , $(\alpha, \epsilon)$ -RDP is $\epsilon$ -DP according to max-divergence. If $\mathcal{M}$ is $\epsilon$ -DP, then $\mathcal{M}$ is $(\alpha, \frac{1}{2}\epsilon^2\alpha)$ -RDP [23].
	$(\epsilon + \frac{\log \frac{1}{\delta}}{\alpha-1}, \delta)$ -DP		If $\mathcal{M}$ is $(\alpha, \epsilon)$ -RDP, then it also satisfies $(\epsilon + \frac{\log \frac{1}{\delta}}{\alpha-1}, \delta)$ -DP.	
Capacity bounded DP [25]	$(\epsilon, \delta)$ -DP	$\mathcal{H}$ -restricted divergence	$D_\Gamma^{\mathcal{H}}(p(z x), p(z x')) \leq \epsilon$	An adversary cannot distinguish between $p(z x)$ and $p(z x')$ beyond $\epsilon$ in the function class $\mathcal{H}$ , where $\Gamma$ is the $f$ -divergence .
	$(\alpha, \epsilon)$ -RDP		An adversary cannot distinguish between $p(z x)$ and $p(z x')$ beyond $\epsilon$ in the function class $\mathcal{H}$ , where $\Gamma$ is the Rényi divergence.	

We compare the other information-theoretic privacy definitions and GDP under the information-theoretic channel model in Table 5. Calmon and Fawaz [26] provided  $\epsilon$ -information privacy, which is stronger than  $2\epsilon$ -DP. Makhdoumi and Fawaz [27] also showed that  $\epsilon$ -information privacy is much stronger than  $2\epsilon$ -DP,  $\epsilon$ -strong DP is stronger than  $\epsilon$ -information privacy, and  $\epsilon$ -DP is stronger than  $(\epsilon, \delta)$ -DP. Wang et al. [12] analyzed the relation between identifiability, DP, and mutual-information privacy and demonstrated that  $\epsilon$ -identifiability is stronger than  $[\epsilon - \max \ln \frac{p(x)}{p(x')}, \epsilon]$ -DP and  $\epsilon$ -DP is stronger than  $[\epsilon, \epsilon + 2 \max \ln \frac{p(x)}{p(x')}]$ -mutual-information privacy. Cuff and Yu [13] also proved that  $\epsilon$ -DP is stronger than  $\epsilon$ -mutual-information DP and  $\epsilon$ -mutual-information DP is stronger than  $(\epsilon, \delta)$ -DP, where  $\epsilon$ -mutual-information DP is  $\epsilon$ -mutual-information privacy of Reference [12].

In the information-theoretic channel model of LDP of Table 3, we use the convex polytope proposed by Holohan et al. [28] as the general definition of the LDP. Thus, the definition of LDP for any different single input  $x$  and  $x'$  and Hamming distance  $\Delta(x, x') = 1$  is

$$\{p(z|x) : e^\epsilon = \max\{\frac{p(z|x)}{p(z|x')}\}\} \quad (5)$$

where  $\sum_z p(z|x) = 1$  and  $p(z|x) \geq 0$ .

In Table 6, we make the comparative analysis of other information-theoretic privacy definitions and LDP under information-theoretic channel model. Jiang et al. [19] compared LDP, mutual-information privacy [12], and local information privacy, where local information privacy is information privacy of Reference [26]. When privacy budget is  $\epsilon$ ,  $\epsilon$ -local information privacy is stronger than  $\epsilon$ -mutual-information privacy and  $2\epsilon$ -LDP, and  $\epsilon$ -LDP is stronger than  $\epsilon$ -local information privacy. Lopuhaä-Zwakenberg et al. [21] also showed the same conclusion above and also proved that  $\epsilon$ -side-channel resistant local information privacy (SRLIP) is stronger than  $\epsilon$ -local information privacy when the privacy budget is  $\epsilon$ .



**Table 5.** Comparative analysis of GDP and other information-theoretic privacy definitions.

Existing Work	Information-Theoretic Privacy Definition	Formula	Description	Relationship to GDP	Stronger or Weaker than GDP
[26]	$\epsilon$ -information privacy	$e^{-\epsilon} \leq \frac{p(x z)}{p(x)} \leq e^\epsilon$	When the output is given, the posterior and prior probabilities of the input $x$ do not change significantly.	$\epsilon$ -information privacy $\Rightarrow$ 2 $\epsilon$ -DP	$\epsilon$ -information privacy is stronger than 2 $\epsilon$ -DP.
[27]	$\epsilon$ -strong DP	$\sup_{z,x,x'} \frac{p(z x)}{p(z x')} \leq e^\epsilon, \forall z, x, x'$	$\epsilon$ -strong DP relaxes the adjacent datasets assumption.	$\epsilon$ -strong DP $\Rightarrow$ $\epsilon$ -information privacy $\epsilon$ -information privacy $\Rightarrow$ 2 $\epsilon$ -strong DP	$\epsilon$ -strong DP is stronger than $\epsilon$ -information privacy. $\epsilon$ -information privacy is stronger than 2 $\epsilon$ -DP. $\epsilon$ -DP is stronger than $(\epsilon, \delta)$ -DP.
	$\epsilon$ -information privacy	The same as above.	The same as above.	$\epsilon$ -information privacy $\Rightarrow$ $\frac{\epsilon}{H(X)}$ -worst-case divergence privacy $\frac{\epsilon}{H(X)}$ -worst-case divergence privacy $\Rightarrow$ $\frac{\epsilon}{H(X)}$ -divergence privacy	
	Worst-case divergence privacy	$H(S) - \min_z H(S Z=z) = \epsilon H(S)$	Some private data $S$ are correlated with some non-private data $X$ .	$\epsilon$ -DP $\Rightarrow$ $(\epsilon, \delta)$ -DP	
[12]	$\epsilon$ -identifiability	$p(x z) \leq e^\epsilon p(x' z)$	Two adjacent datasets cannot be distinguished from the posterior probabilities after observing the output dataset, which makes any individual's data hard to identify.	$\epsilon$ -identifiability $\Rightarrow$ $[\epsilon - \max \ln \frac{p(x)}{p(x')}, \epsilon]$ -DP	$\epsilon$ -identifiability is stronger than $[\epsilon - \max \ln \frac{p(x)}{p(x')}, \epsilon]$ -DP.
	$\epsilon$ -mutual-information privacy	$I(X; Z) \leq \epsilon$	Mutual-information privacy measures the average amount of information about $X$ contained in $Z$ .	$\epsilon$ -DP $\Rightarrow$ $[\epsilon, \epsilon + 2 \max \ln \frac{p(x)}{p(x')}]$ -mutual-information privacy	$\epsilon$ -DP is stronger than $[\epsilon, \epsilon + 2 \max \ln \frac{p(x)}{p(x')}]$ -mutual-information privacy.
[13]	$\epsilon$ -mutual-information DP	$\sup_{p(x_i)} I(x_i; Z X^{-i}) \leq \epsilon$	The same as $\epsilon$ -mutual-information privacy in work [12] above, and $X^{-i}$ represents the input dataset except the $i$ -th element.	$\epsilon$ -DP $\Rightarrow$ $\epsilon$ -mutual information DP $\Rightarrow$ $(\epsilon, \delta)$ -DP	$\epsilon$ -DP is stronger than $\epsilon$ -mutual-information DP. $\epsilon$ -mutual-information DP is stronger than $(\epsilon, \delta)$ -DP.

**Table 6.** Comparative analysis of LDP and other information-theoretic privacy definitions.

Existing Work	Information-Theoretic Privacy Definition	Formula	Description	Relationship to LDP	Stronger or Weaker than LDP
[12,19]	$\epsilon$ -mutual-information privacy	The same as Table 5 above.	The same as Table 5 above.	$\epsilon$ -local information privacy $\Rightarrow$ $\epsilon$ -mutual-information privacy	$\epsilon$ -local information privacy is stronger than 2 $\epsilon$ -LDP.
[19,26]	$\epsilon$ -local information privacy			$\epsilon$ -local information privacy $\Rightarrow$ 2 $\epsilon$ -LDP $\epsilon$ -LDP $\Rightarrow$ $\epsilon$ -local information privacy	$\epsilon$ -LDP is stronger than $\epsilon$ -local information privacy.
[21,26]	$\epsilon$ -local information privacy	The same as Table 5 above.	The same as Table 5 above.	$\epsilon$ -LDP $\Rightarrow$ $\epsilon$ -local information privacy	$\epsilon$ -LDP is stronger than $\epsilon$ -local information privacy.
[21]	$\epsilon$ -SRLIP	$e^{-\epsilon} \leq \frac{p(z s,x_1,\dots,x_m)}{p(z x_1,\dots,x_m)} \leq e^\epsilon$	SRLIP satisfies $\epsilon$ -LIP for the attacker accessing some data $\{x_1, \dots, x_m\}$ of a user and does not leak sensitive data $s$ beyond the knowledge the attacker gained from the side channel.	$\epsilon$ -local information privacy $\Rightarrow$ 2 $\epsilon$ -LDP $\epsilon$ -SRLIP $\Rightarrow$ $\epsilon$ -local information privacy	$\epsilon$ -local information privacy is stronger than 2 $\epsilon$ -LDP.

## 5. Privacy-Utility Metrics of GDP and LDP under Information-Theoretic Channel Models

In Table 7, we summarize and analyze the information-theoretic privacy metrics of GDP. When  $\alpha \rightarrow \infty$ , Rényi divergence is used as the privacy metric of GDP, which is a natural relaxation of GDP based on the Rényi divergence [11]. Chaudhuri et al. [25] used restricted divergences  $D_{\Gamma}^H(p(z|x), p(z|x'))$  as privacy metric. When  $\Gamma$  is Rényi divergence, the capacity bounded DP is a generalization of RDP. When  $\Gamma$  is  $f$ -divergence, the capacity bounded DP is  $(\epsilon, \delta)$ -DP in [8]. In [14,29], mutual information is used as the privacy metric of GDP, which is the amount of information leaked on  $X$  after observing  $Z$ . Cuff and Yu [13] also used  $\alpha$ -mutual-information as the privacy metric of GDP, which is the generalization of mutual information using Rényi divergence of order  $\alpha$ . Alvim et al. [7] used min-entropy leakage as the privacy metric of GDP, which is the ratio of the probabilities of right guessing a priori and a posterior. Furthermore, maximal leakage of channel  $p(z|x)$  is used as the privacy metric of GDP, which is the maximal reduction in uncertainty of  $X$  when  $Z$  is given [7,16]. According to the graph symmetrization, Edwards et al. [30] also regarded min-entropy leakage as an important measure of differential privacy loss of information channels under Blowfish privacy. Blowfish privacy is a generalization of global differential privacy. Rogers et al. [31] defined the privacy metric of GDP using max-information and  $\beta$ -approximate max-information, which are a correlation measure allowing to bound the change in the conditional probability of an event relative to the prior probability. In [32,33], the privacy budget is directly used as privacy metric. Therefore, we can conclude that Rényi divergence is a more general privacy metric of GDP, since Rényi divergence is a generalization of restricted divergences and it can deduce  $f$ -divergence, min-entropy leakage, maximal leakage, and max-information. Moreover, mutual information can also be used as a privacy metric of GDP.

We also summarize and analyze the information-theoretic utility metrics of GDP in Table 8. In the information-theoretic channel model of GDP, expected distortion is mainly the utility measurement method, which shows how much information about the real answer can be obtained from the reported answer to average [7,33]. Padakandla et al. [32] used fidelity as the utility metric, and the fidelity between transition probability distributions is measured by  $\mathbb{L}_1$ -distortion metric. Mutual information is not only used as a privacy metric but also as a utility metric of GDP, which captures the amount of information shared by two variables [33].

In Table 9, we summarize and analyze existing work of information-theoretic privacy metrics of LDP. In the information-theoretic channel model of LDP, Duchi et al. [17] defined the privacy metric of LDP using KL-divergence, which bounds the KL-divergence between distributions  $p(z|x)$  and  $p(z|x')$  by a quantity dependent on the privacy budget  $\epsilon$  and gives the upper bound of KL-divergence by combining with the total variation distance between  $p_1(x_i)$  and  $p_2(x_i)$  of the initial distributions of the  $x_i$ . Of course, mutual information can also be used as a privacy measure of LDP [34,35]. More generally, the existing work mainly uses the definition of the LDP as the privacy metric [5,36–38]. In [39], Lopuhaä-Zwakenberg et al. gave an average privacy metric based on the ratio of conditional entropy of sensitive information  $X$ .

Next, we summarize and analyze the information-theoretic utility metric of LDP in Table 10. In the information-theoretic channel model of LDP,  $f$ -divergence [5] and mutual information [5,36,38] can also be used as utility measures of LDP. In most cases, expected distortion is used as the utility measure of LDP [20,34–37]. In [39], Lopuhaä-Zwakenberg et al. presented distribution utility and tally utility metrics based on the ratio of relevant information.

**Table 7.** Privacy metrics of GDP under information-theoretic channel model.

Existing Work	Privacy Metric	Formula	Description	Bound
[16]	Maximal leakage	$ML(p(z x)) = \max_{p(x)}(H_\infty(X) - H_\infty(X Z))$	The maximal leakage of channel $p(z x)$ is the maximal reduction in uncertainty of $X$ when $Z$ is given, which is taken by maximizing over all input distributions of the attacker's side information.	$ML(p(z x)) \leq d\epsilon \log_2 e + \log_2 m$ with spheres $\{x \in \{0, 1\}^n   d(x, x_i) \leq d\}$ of radius $d$ and center $x_i$ .
[7]	Min-entropy leakage	$I_\infty(X; Z) = H_\infty(X) - H_\infty(X Z)$	The min-entropy leakage corresponds to the ratio between the probabilities of attack success with a priori and a posterior.	$I_\infty(X; Z) \leq n \log_2 \frac{v\epsilon^e}{v-1+\epsilon^e}$ with $v \geq 2$
	Worst-case leakage	$C_\infty = \max_{p(x)} I_\infty(X; Z)$	The same as maximal leakage above.	
[29]	Mutual information	$I(X; Z)$	The mutual information denotes the amount of information leaked on $X$ given $Z$ .	$I(X; Z) \leq 3\epsilon n$ $I(X; Z) \geq n(1 - 2\eta)$ with $\delta \geq 2^{-C(\epsilon, \eta)n}$ , $0 < \epsilon, \eta < 1$ , and a constant $C(\epsilon, \eta) > 0$
[30]	Min-entropy leakage	The same as above.	The same as above.	$I_\infty(X; Z) \leq \log(\sum_{t=1}^q \exp(\epsilon d_t))$ , where $q$ is the number of connected components of induced adjacency graph, and $d_t$ is the diameter of the $t$ -th connected component.
[14]	Mutual information	$I(X; Z)$	The same as above.	–
[13]	$\alpha$ -mutual-information	$I_\alpha(X; Z) = \min_{p(z)} D_\alpha(p(z x)    p(z)p(x))$	The notion of $\alpha$ -mutual-information is the generalization of mutual information using Rényi information measures.	$\sup_{p(x_i)} I_\alpha(x_i; Z   X^{-i}) \leq \epsilon$
[31]	Max-information	$I_\infty(X; Z) = \log_2 \sup_{x, z \in (X, Z)} \frac{p(x, z)}{p(x)p(z)}$	Maximum information is a correlation measure, similar to mutual information, which allows to bound the change of the conditional probability of an event relative to prior probability.	$I_\infty(X; Z) \leq \log_2 e \cdot \epsilon n$ and $I_\infty^\beta(X; Z) \leq \log_2 e \cdot (\epsilon^e \frac{n}{2} + \epsilon \sqrt{\frac{n \ln \frac{2}{\beta}}{2}})$ for $\epsilon$ -DP $I_\infty^\beta(X; Z) = O(n\epsilon^2 + n\sqrt{\frac{\epsilon}{\beta}})$ for $(\epsilon, \delta)$ -DP
	$\beta$ -approximate max-information	$I_\infty^\beta(X; Z) = \log_2 \sup_{O \subseteq (X \times Z), p((x, z) \in O) > \beta} \frac{p((x, z) \in O) - \beta}{p(x)p(z)}$		
[11]	Rényi divergence	$D_\alpha(p(z x)    p(z x'))$	A natural relaxation of GDP based on the Rényi divergence.	–
[25]	$\mathcal{H}$ -restricted divergences	$D_\Gamma^{\mathcal{H}}(p(z x), p(z x'))$	The privacy loss is measured in terms of a divergence $\Gamma$ between output distributions of a mechanism on datasets that differ by a single record restricted to functions in $\mathcal{H}$ .	$D_{\text{KL}}^{\mathcal{H}}(p(z x), p(z x')) \leq 8\sqrt{\epsilon}$
[32,33]	Privacy budget	$\epsilon = \ln \frac{p(z x)}{p(z x')}$	The privacy budget represents the level of privacy preserving.	–

**Table 8.** Utility metrics of GDP under information-theoretic channel model.

Existing Work	Utility Metric	Formula	Description	Bound
[7]	Expected distortion	$U(Y, Z) = \sum_y \sum_z p(y)p(z y)d(y, z)$	How much information about the real answer can be obtained from the reported answer to average.	$U(Y, Z) \leq \frac{e^{\epsilon n} (1 - e^\epsilon)}{e^{\epsilon n} (1 - e^\epsilon) + c(1 - e^{\epsilon n})}$ with $ \{z d(y, z) = d\}  = c$
[14]	Expected distortion	$\sum_x \sum_z p(x)p(z x)d(x, z)$	The same as above.	–
[32]	Fidelity	$\ \cdot\ _1$	The fidelity of a pair of transition probability distributions is $\mathbb{L}_1$ -distortion metric.	–
[33]	Mutual information	$I(X; Z)$	Mutual information captures the amount of information shared by two variables, that is to say, quantifying how much information can be preserved when releasing a private view of the data.	–

**Table 9.** Privacy metrics of LDP under information-theoretic channel model.

Existing Work	Privacy Metric	Formula	Description	Bound
[17]	KL-divergence	$D_{KL}(p(z x)  p(z x'))$	The general result bounds the KL-divergence between distributions $p(z x)$ and $p(z x')$ by the privacy budget $\epsilon$ and the total variation distance between $p(x)$ and $q(x)$ of the initial distributions of the X.	$D_{KL}(p(z x)  p(z x')) + D_{KL}(p(z x')  p(z x)) \leq 4(e^\epsilon - 1)^2 \ p(x) - q(x)\ _{TV}^2$
[34,35]	Mutual information	$I(X; Z)$	The same as Table 7 above.	–
[4,5,37,38]	Privacy budget	$\epsilon = \ln \frac{p(z x)}{p(z x')}$	The same as Table 7 above.	–
Average privacy [39]	Conditional entropy	$\frac{H(X Z, P)}{H(X P)}$	Privacy metric is the fraction of sensitive information that is retained from the aggregator with prior knowledge $P$ .	–

**Table 10.** Utility metrics of LDP under information-theoretic channel model.

Existing Work	Utility Metric	Formula	Description	Bound
[34,35,37]	Expected Hamming distortion	$E[d(x, z)] = p(x \neq z) = \sum_x \sum_z p(x)p(z \neq x x)$	Hamming distortion measures the utility of a channel $p(z x)$ in terms of the worst-case Hamming distortion over source distribution $p(x)$ .	-
[5]	$f$ -divergence	$D_f(p(z x)  p(z x')) = \sum_x p(z x')f(\frac{p(z x)}{p(z x')})$	$f$ -divergence measures statistical discrimination between distributions $p(z x)$ and $p(z x')$ by the privacy budget $\epsilon$ and the total variation distance between $p(x)$ and $q(x)$ of the initial distributions of the $X$ .	$D_{KL}(p(z x)  p(z x')) + D_{KL}(p(z x')  p(z x)) \leq \frac{2(1+\delta)(\epsilon-1)^2}{\epsilon^{\delta+1}}   p(x) - q(x)  _{TV}^2$
	Mutual information	$I(X; Z)$	The same as Table 8 above.	$I(X; Y) \leq \frac{1}{2}(1 + \delta)P(T)P(T^c)\epsilon^2$ with $T \in \arg \min_{A \subseteq X}  P(A) - \frac{1}{2} $ for a given distribution $P$ and partitioning $X$ into two parties $T$ and $T^c$
[36]	Expected distortion	$\sum_x \sum_z p(x)p(z x)d(x, z)$	A channel $p(z x)$ yields a small distortion between input and output sequences with respect to a given distortion measure.	-
Average error probability [20]	Expected Hamming distortion	$p_E = \sum_x p(x) \sum_{x \neq z} p(z x)$	The average error probability is defined to be the expected Hamming distortion between the input and output data based on maximum a posterior estimation.	$p_E = \frac{n-1}{n-1+\epsilon^n}$
[38]	Mutual information	$I(X; Z)$	The same as Table 8 above.	$\sup_{p(z x)} I(X; Z) = \max_{k=\lfloor \beta \rfloor}^{\lceil \beta \rceil} \{ \frac{k \cdot \epsilon^n \log \frac{m \cdot \epsilon^n}{k \cdot \epsilon^n + m - k} \log \frac{m}{k \cdot \epsilon^n + m - k}}{k \cdot \epsilon^n + m - k} \}$ with $\beta = \frac{(\epsilon^n - \epsilon^n + 1)m}{(\epsilon^n - 1)^2}$
Distribution utility [39]	Mutual information	$\frac{I(Z; P)}{I(X; P)}$	Utility metric is the fraction of relevant information after accessing to prior knowledge $P$ or tally vector $T = (T_x)_{x \in X}$ and $T_x =  \{i : x_i = x\} $ .	-
Tally utility [39]	Entropy Mutual information	$\frac{I(Z; T)}{H(T)}$		

## 6. Properties of GDP and LDP under Information-Theoretic Channel Models

In Table 11, we present and analyze the properties of GDP based on the information-theoretic channel model. According to the Rényi divergence, Mironov [11] demonstrated that the new definition shares many important properties with the standard definition of GDP, including post-processing, group privacy, and sequential composition. Considering  $\mathcal{H}$ -restricted divergences including Rényi divergence, Chaudhuri et al. [25] showed that capacity bounded DP has properties of post-processing, convexity, sequential composition, and parallel composition. Barthe and Köpf [16] proved the sequential composition and parallel composition of GDP based on maximal leakage under the information-theoretic channel model. Barthe and Olmedo [8] also proved the parallel composition of GDP using  $f$ -divergence. We know that Rényi divergence can deduce maximal leakage and max-divergence.  $f$ -divergence of Reference [8] is actually max-divergence. Thus, we can conclude that, such as post-processing, convexity, group privacy, and sequential composition, and parallel composition, the properties of GDP can be proved by using Rényi divergence.

Similarly, GDP and LDP share the above properties under the information-theoretic channel model. Therefore, LDP also has the properties of post-processing, convexity, group privacy, and sequential composition, and parallel composition.

Moreover, we have showed that GDP and LDP have privacy-utility monotonicity [3]. In GDP,  $(\epsilon, \delta)$ -DP shows

$$\frac{p(z|x) - \delta}{p(z)} = \frac{p(z|x) - \delta}{\sum_{x'} p(z|x')p(x')} \leq \frac{p(z|x) - \delta}{\sum_{x'} (p(z|x) - \delta)p(x')e^{-\epsilon}} = e^\epsilon \quad (6)$$

We can obtain

$$\sum_x \sum_z p(xz) \log \frac{p(z|x) - \delta}{p(z)} \leq \epsilon \leq I(X; Z) \quad (7)$$

When  $\delta = 0$ , we have

$$I(X; Z) = \sum_x \sum_z p(xz) \log \frac{p(z|x)}{p(z)} \leq \epsilon \quad (8)$$

We can obtain  $I(X; Z) = \epsilon$ . We use mutual information as the utility metric. We can conclude that the mutual information of GDP decreases as the decreasing of the privacy budget, and vice versa. Privacy preserving is stronger and the utility is worse, and vice versa. Thus, GDP has privacy-utility monotonicity indicating the privacy-utility tradeoff. Similarly, we can observe that LDP also has privacy-utility monotonicity indicating the privacy-utility tradeoff.

**Table 11.** Properties of GDP under information-theoretic channel model.

Existing Work	Privacy Type	Privacy Property	Information-Theoretic Metric	Formal Description
[16]	GDP	Sequential composition	Maximal leakage	$ML(C_1 + C_2) \leq ML(C_1) + ML(C_2)$ for the sequential composition $C_1 + C_2$ of channels $C_1$ and $C_2$ . When $C_1$ is $\epsilon_1$ -DP and $C_2$ is $\epsilon_2$ -DP, $C_1 + C_2$ is $\epsilon_1 + \epsilon_2$ -DP.
		Parallel composition		$ML(C_1 \times C_2) = ML(C_1) + ML(C_2)$ for the parallel composition $C_1 \times C_2$ of channels $C_1$ and $C_2$ . When $C_1$ is $\epsilon_1$ -DP and $C_2$ is $\epsilon_2$ -DP, $C_1 \times C_2$ is $\max\{\epsilon_1, \epsilon_2\}$ -DP.
[8]	GDP	Sequential composition	$f$ -divergence	$\Delta_{\alpha\alpha'}(p(z x), p(z x')) \leq \Delta_\alpha(p(z x), p(z x')) + \max_x \Delta_{\alpha'}(p(z x), p(z x'))$ , where $\Delta_{\alpha'}$ , the same as Table 4 above.
[11]	RDP	Post-processing	Rényi divergence	If there is a randomized mapping $g : R \rightarrow R'$ , then $D_\alpha(p(z x)  p(z x')) \geq D_\alpha(g(p(z x))  g(p(z x')))$ .
		Group privacy		If $\mathcal{M} : x \rightarrow R$ is $(\alpha, \epsilon)$ -RDP, $g : x' \rightarrow x$ is $2^c$ -stable and $\alpha \geq 2^{c+1}$ , then $\mathcal{M} \circ g$ is $(\frac{\alpha}{2^c}, 3^c \epsilon)$ -RDP.
		Sequential composition		If $\mathcal{M}_1 : x \rightarrow R_1$ is $(\alpha, \epsilon_1)$ -RDP and $\mathcal{M}_2 : R_1 \times x \rightarrow R_2$ is $(\alpha, \epsilon_2)$ -RDP, then the mechanism $(\mathcal{M}_1, \mathcal{M}_2)$ satisfies $(\alpha, \epsilon_1 + \epsilon_2)$ -RDP.
[25]	Capacity bounded DP	Post-processing	$\mathcal{H}$ -restricted divergences	$\mathcal{H}, \mathcal{G}$ , and $\mathcal{I}$ are function classes such that for any $g \in \mathcal{G}$ and $i \in \mathcal{I}$ , $i \circ g \in \mathcal{H}$ . If mechanism $\mathcal{M}$ is $(\mathcal{H}, \Gamma)$ -capacity bounded DP with $\epsilon$ , then $g \circ \mathcal{M}$ is also $(\mathcal{I}, \Gamma)$ -capacity bounded DP with $\epsilon$ for any $g \in \mathcal{G}$ .
		Convexity		$\mathcal{M}_1$ and $\mathcal{M}_2$ are two mechanisms which have the same range and provide $(\mathcal{H}, \Gamma)$ -capacity bounded DP with $\epsilon$ . If $\mathcal{M}$ is a mechanism which executes mechanism $\mathcal{M}_1$ with probability $\pi$ and $\mathcal{M}_2$ with probability $1 - \pi$ , then $\mathcal{M}$ is $(\mathcal{H}, \Gamma)$ -capacity bounded DP with $\epsilon$ .
		Sequential composition		$\mathcal{H}$ is the function class $\mathcal{H} = \{\mathcal{H}_1 + \mathcal{H}_2   h_1 \in \mathcal{H}_1, h_2 \in \mathcal{H}_2\}$ . If $\mathcal{M}_1(x)$ and $\mathcal{M}_2(x)$ are $(\mathcal{H}_1, \Gamma)$ and $(\mathcal{H}_2, \Gamma)$ capacity bounded DP with $\epsilon_1$ and $\epsilon_2$ , respectively, then the combination $(\mathcal{M}_1, \mathcal{M}_2)$ is $(\mathcal{H}, \Gamma)$ capacity bounded DP with $\epsilon_1 + \epsilon_2$ .
		Parallel composition		$\mathcal{H}$ is the function class $\mathcal{H} = \{\mathcal{H}_1 + \mathcal{H}_2   h_1 \in \mathcal{H}_1, h_2 \in \mathcal{H}_2\}$ . If $\mathcal{M}_1(x_1)$ and $\mathcal{M}_2(x_2)$ are $(\mathcal{H}_1, \Gamma)$ and $(\mathcal{H}_2, \Gamma)$ capacity bounded DP with $\epsilon_1$ and $\epsilon_2$ respectively, and the datasets $x_1$ and $x_2$ are disjoint, then the combination $(\mathcal{M}_1(x_1), \mathcal{M}_2(x_2))$ is $(\mathcal{H}, \Gamma)$ capacity bounded DP with $\max\{\epsilon_1, \epsilon_2\}$ .
[3]	GDP LDP	Privacy-utility monotonicity	Mutual information	The mutual information decreases as the decreasing of the privacy budget, and vice versa

## 7. GDP and LDP Mechanisms under Information-Theoretic Channel Models

In Table 12, we summarize and compare the GDP mechanisms from the perspective of information-theoretic channel on uniform distribution of the source  $X$ . Alvim et al. [7] maximized expected distortion under min-entropy leakage constraint and obtained the optimal randomization mechanism using graph symmetry caused by the adjacent relationship between adjacent datasets. The optimal randomization mechanism can ensure better utility while achieving  $\epsilon$ -DP. According to the risk-distortion framework, Mir [14] minimized mutual information when the constraint condition is expected distortion and obtain  $\epsilon$ -DP mechanism  $p(z|x) = \frac{p(z) \exp(-\epsilon d(x,z))}{Z(x,\epsilon)}$  by Lagrangian multipliers method, where  $Z(x,\epsilon)$  is a normalization function. GDP mechanism of [14] is corresponding to the exponential mechanism [40]. The conditional probability distribution  $p(z|x)$  minimizes the privacy leakage risk given a distortion constraint. Ayed et al. [33] maximized mutual information when constraint condition is DP and solved the constrained maximization program to obtain DP mapping under strongly symmetric channel.

In addition, Mironov [11] analyzed the RDP of three basic mechanisms and their self-composition, including randomized response, Laplace mechanism, and Gaussian mechanism, and gave the parameters of RDP of these mechanisms. Considering a linear adversary and unrestricted adversary, Chaudhuri et al. [25] also discussed the capacity bounded DP properties of Laplace mechanism, Gaussian mechanism, and matrix mechanism and presented the bound of privacy budget  $\epsilon$  of Laplace mechanism and Gaussian mechanism under KL-divergence and Rényi divergence, respectively.

In Table 13, we summarize and compare the LDP mechanisms from the perspective of information-theoretic channel under uniform distribution of the source  $X$ . According to the rate-distortion function, References [34,35,37] maximized mutual information under expected Hamming distortion  $D$  constraint and obtained privacy budget  $\epsilon = \log \frac{1-D}{D}$  for binary channel and privacy budget  $\epsilon = \log(m-1) + \frac{1-D}{D}$  for discrete alphabets. Kairouz et al. [5] maximized KL-divergence and mutual information under LDP constraint and obtained binary randomized response mechanism, multivariate randomized response mechanism, and quaternary randomized response mechanism by solving the privacy-utility maximization problem, which is equivalent to solving the finite-dimensional linear program. Although Ayed et al. [33] maximized mutual information about GDP constraint, they also obtained binary randomized response mechanism and multivariate randomized response mechanism under a strongly symmetric channel. Wang et al. [38] maximized mutual information on LDP constraint and obtained the  $k$ -subset mechanism with respect to the uniform distribution on the source  $X$ . When  $k = 1$ , the 1-subset mechanism is the multivariate randomized response mechanism. When  $n = 2$  and  $k = 1$ , the multivariate randomized response mechanism is the binary randomized response mechanism. Xiong et al. [36] minimized privacy budget  $\epsilon = \max_{x,x',z} \frac{p(z|x)}{p(z|x')}$  under expected distortion constraint, which is equivalent to solving a standard generalized linear-fractional program via the bisection method. However, Xiong et al. [36] did not give a specific expression of the optimal privacy channel  $p(z|x)$ .



**Table 12.** GDP mechanisms under information-theoretic channel model.

Existing Work	Privacy Type	Model	Objective Function	Constraint Condition	Mechanism	Solution	Description
[7]	GDP	Maximal utility	Expected distortion $U(Y, Z) = \sum_y \sum_z p(y)p(z y)d(y, z)$	Min-entropy leakage $I_\infty(X; Z) = H_\infty(X) - H_\infty(X Z)$	$p(z y) = \frac{\alpha}{(\alpha^d)^y}$ , where $d = d(y, z)$ , $\alpha = \frac{(\epsilon^y)(1-\epsilon^d)}{(\epsilon^y)^n(1-\epsilon^d)^n + c(1-(\epsilon^d)^n)}$ , and $c$ the same as Table 8 above.	Graph symmetry induced by the adjacent relationship of adjacent datasets.	Optimal randomization mechanism provides the better utility while guaranteeing $\epsilon$ -DP.
[14]	GDP	Risk-distortion	Mutual information $\inf_{p(z x)} I(X; Z)$	Expected distortion $\sum p(x) \sum p(z x)d(x, z) \leq D$	$p(z x) = \frac{p(z) \exp(-\epsilon d(x, z))}{Z(x, \epsilon)}$ , where $Z(x, \epsilon)$ is a normalization function.	Lagrangian multipliers.	Conditional probability distribution is DP mapping, which minimizes the privacy risk given a distortion constraint.
[33]	GDP	Constrained maximization program	Mutual information $\max I(X; Z)$	GDP $\sup \frac{p(z x)}{p(z x')} \leq \exp(\epsilon)$	$p(z x) = \begin{cases} p(z = x x), & x = z \\ \frac{1-p(z=x x)}{m-1}, & x \neq z \end{cases}$	Definition of GDP.	When $x$ is transformed into $z$ and $z = x$ , the conditional transition probability is $p(z = x x)$ . When $z \neq x$ , the conditional transition probability is $\frac{1-p(z=x x)}{m-1}$ under strongly symmetric channel.

**Table 13.** LDP mechanisms under information-theoretic channel model.

Existing Work	Privacy Type	Model	Objective Function	Constraint Condition	Mechanism	Solution	Description
[34,35,37]	LDP	Rate-distortion function	Mutual information $\min_{p(z x)} I(X; Z)$	Expected Hamming distortion $\sum_x \sum_z p(x)p(z x)d(x, z) \leq D$	Binary channel Discrete alphabet	$\epsilon = \log \frac{1-D}{D}$ $\epsilon = \log(m-1) + \log \frac{1-D}{D}$	Memoryless symmetric channel.
[5]	LDP	Constraint maximization problem	KL-divergence Mutual information $\max_{p(z x)} D_{KL}(p(z x)  p(z x'))$ $\max_{p(z x)} I(X; Z)$	LDP $\epsilon = \ln \frac{p(z x)}{p(z x')}$	Binary randomized response Multivariate randomized response Quaternary randomized response	$p(z x) = \begin{cases} \frac{\epsilon^x}{1+\epsilon^x}, & x = z \\ \frac{1}{1+\epsilon^x}, & x \neq z \end{cases}$ $p(z x) = \begin{cases} \frac{\epsilon^x}{n-1+\epsilon^x}, & x = z \\ \frac{1}{n-1+\epsilon^x}, & x \neq z \end{cases}$ $\begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & \delta & 0 & \frac{1-\delta}{1+\epsilon^\delta} & \frac{(1-\delta)\epsilon^\delta}{1+\epsilon^\delta} \\ 1 & 0 & \delta & \frac{(1-\delta)\epsilon^\delta}{1+\epsilon^\delta} & \frac{1-\delta}{1+\epsilon^\delta} \end{pmatrix}$	Solving the privacy-utility maximization problem is equivalent to solving finite-dimensional linear program.
[38]	LDP	Maximize utility	Mutual information $\sup_{p(z x)} I(X; Z) \leq I_\beta$ $I_k = \frac{k\epsilon^k \log \frac{\epsilon^k}{\epsilon^k + m - k} \log \frac{\epsilon^k + m - k}{\epsilon^k + m - k - 1}}{k\epsilon^k + m - k}$ $\beta = \frac{(\epsilon^k - \epsilon^{k+1})^m}{(\epsilon - 1)^2}$	LDP $\epsilon = \ln \frac{p(z x)}{p(z x')}$	$k$ -subset mechanism	$p(Z x) = \begin{cases} \frac{n\epsilon^k}{\binom{n}{k}(k\epsilon^k + n - k)}, &  Z  = k, x \in Z \\ \frac{n}{\binom{n}{k}(k\epsilon^k + n - k)}, &  Z  = k, x \notin Z \\ 0, &  Z  \neq k \end{cases}$	This problem maximizes mutual information when $x$ is a sample according to the uniform distribution with probability $\frac{1}{n}$ .

Furthermore, Duchi et al. [41] showed that randomized response is an optimal way to perform survey sampling while maintaining privacy of the respondents. Holohan et al. [42] proposed following optimal mechanism of randomized response satisfying  $(\epsilon, \delta)$ -DP under uniform distribution of the source  $X$ , which is

$$p(z|x) = \begin{cases} \frac{e^\epsilon + \delta}{1 + e^\epsilon}, & x = z \\ \frac{1 - \delta}{1 + e^\epsilon}, & x \neq z \end{cases} \quad (9)$$

Erlingsson et al. [43] proposed randomized aggregatable privacy-preserving ordinal response (RAPPOR) by applying randomized response in a novel manner. RAPPOR provides privacy guarantee using permanent randomized response and instantaneous randomized response and ensures high-utility analysis of the collected data. RAPPOR encodes each value  $v$  into a length- $k$  binary bit vector  $B$ . For permanent randomized response, RAPPOR generates  $B_1$  with the probability

$$p(B_1[v] = 1) = \begin{cases} 1 - \frac{1}{2}f, & B[v] = 1 \\ \frac{1}{2}f, & B[v] = 0 \end{cases} \quad (10)$$

where  $f = \frac{2}{e^{\frac{\epsilon}{2}} + 1}$ . With respect to instantaneous randomized response, RAPPOR perturbs  $B_1$  with the probability

$$p(B^*[i] = 1) = \begin{cases} p, & B_1[i] = 1 \\ q, & B_1[i] = 0 \end{cases} \quad (11)$$

## 8. Differential Privacy Synthetic Data Generation

Data sharing facilitates training better models, decision making, and the reproducibility of scientific research. However, if the data are shared directly, it will face the risk of privacy leakage and the problem of small training sample size. Thus, synthetic data are often used to replace the sharing of real data. At present, one of the main methods for synthetic data generation is generative adversarial network [44]. GAN consists of two neural networks: one is a generator, and the other is a discriminator. The generator generates a realistic sample by inputting a noise obeying multivariable Gaussian distribution or uniform distribution. The discriminator is a binary classifier (such as 0–1 classifier) to judge whether the input sample is real or fake. In other words, the discriminator can distinguish whether each input sample comes from the real sample set or the fake sample set. However, the generator makes the ability of making samples as strong as possible so that the discriminator cannot judge whether the input sample is a real sample or a fake sample. According to this process, GAN can generate synthetic data to approximate the real data. Because the synthetic data accurately reflect the distribution of training data, it can avert privacy leakage by replacing real data sharing, augment small-scale training data, and be generated as desired. Thus, GAN can generate synthetic data for time series, continuous, and discrete data [45].

However, because the discriminator easily memorizes the training data, it brings the risk of privacy leakage [46]. Therefore, GAN mainly faces the privacy threat of membership inference attack and model extraction attack in Table 14. Hayes et al. [47] proposed a membership inference attack against the generative models, which means that the attacker can determine whether it is used to train the model given a data point. Liu et al. [48] proposed a new membership inference attack, co-membership inference attack, which checks whether the given  $n$  instances are in the training data, where the prior knowledge is completely used or not at all in the training. Hilprecht et al. [49] proposed a Monte Carlo attack on the membership inference against generative models, which yields high membership inference accuracy. Chen et al. [50] systematically analyzed the potential risk of privacy leakage caused by the generative models and proposed the classification

of membership inference attacks, including not only the existing attacks but also the proposed generic attack model based on reconstruction. Hu and Pang [51] studied the model extraction attack against GAN by stealing the machine learning model whose purpose is to copy the machine learning model through query access to the target model. In order to mitigate the model extraction attack, Hu and Pang designed defenses based on input and output perturbation by perturbing latent code and generating samples, respectively.

However, the existing work mainly achieves the model protection of neural network based on differential privacy. By using the  $\ell_2$  norm of the gradient and the clipping threshold to clip the gradient, and using the Gaussian mechanism to randomly perturb the clipping gradient, Abadi et al. [52] proposed differential privacy stochastic gradient decent (DP-SGD) to protect the privacy of training data during the training process and demonstrated the moment accountant of the privacy loss that provides a tighter bound on the privacy loss compared to the generic strong composition theorem of differential privacy [9].

Next, in Tables 15 and 16, we mainly review the work of synthetic data generation based on differential privacy GAN and differential privacy GAN with federated learning from the following aspects: gradient perturbation, weight perturbation, data perturbation, label perturbation, and objective function perturbation. Thus, our work is different from the existing surveys [53,54].

#### *8.1. Differential Privacy Synthetic Data Generation with Generative Adversarial Network*

Because the discriminator of GAN can easily remember the training samples, training GAN with sensitive or private data samples breaches the privacy of the training data. Thus, using gradient perturbation can protect the privacy of the sensitive training data by training GAN models with differential privacy based on DP-SGD. Existing work protects the privacy of the training dataset by adding carefully designed noise to clipping gradients during the learning procedure of discriminator and uses moment accountant or RDP accountant to better keep track of the privacy cost for improving the quality of synthetic data. RDP accountant [11] provides a tighter bound for privacy loss in comparison with the moment accountant. In gradient perturbation, clipping strategy and perturbation strategy improve the performance of the model while preserving privacy of the training dataset.

**Table 14.** Membership inference attack and model extraction attack against GAN.

Existing Work	Attack Target	Attack Type	Attack Method	Characteristic	Attack Effect
[47]	Generative models	Membership inference	The discriminator can learn the statistical difference of distribution, detect overfitting and recognize the input as part of the training dataset.	The proposed attack has low running cost, does not need information about the attacked model, and has good generalization.	Defenses are either ineffective or lead to a significant decline in the performance of the generative models in terms of training stability or sample quality.
[48]	Generative models	Co-membership inference	The membership inference of the target data $x$ is used as the optimization of the attacker's network to search for potential codes to reproduce $x$ , and the final reconstruction error is used to judge whether $x$ is in the training data.	When the generative models are trained with large datasets, the co-membership inference attack is necessary to achieve success.	The performance of attacker's network is better than that of previous membership attacks, and the power of co-membership attack is much greater than that of a single attack.
[49]	Generative models	Membership inference	The membership inference attack based on Monte Carlo integration only considers the small distance samples in the model.	This attack allows membership inference without assuming the type of generative models.	The success rate of this attack is better than that of previous studies on most datasets, and there are only very mild assumptions.
[50]	Generative models	Membership inference	This work proposed a general attack model based on reconstruction for which the model is suitable for all settings according to the attacker's knowledge about the victim model.	This work provides a theoretically reliable attack calibration technology, which can continuously improve the attack performance in different attack settings, data modes, and training configurations in all cases.	This attack reveals the information of the training data used for the victim model.
[51]	GAN	Model extraction	This work studied the model extraction attack based on target and background knowledge from the perspectives of fidelity extraction and accuracy extraction.	Model extraction based on transfer learning can enable adversaries to improve the performance of their GAN model through transfer learning.	Attack model stealing the most advanced target model can be transferred to new fields to expand the application scope of extraction model.

Using gradient perturbation, Lu and Yu [55] proposed a unified framework for publishing differential privacy data based on GAN, such as tabular data and graphs, and synthetic data with acceptable utility in differential privacy manner. Xie et al. [56] proposed a differential privacy Wasserstein GAN (WGAN) [57] model, which adds carefully designed noise to the clipping gradient in the learning process, generates high-quality data points at a reasonable privacy level, and uses moment accountant to ensure the privacy in the iterative gradient descent process. Frigerio et al. [45] developed a differential privacy framework for privacy protection data publishing using GAN, which can easily adapt to the generation of continuous, time series, and discrete data and maintain the original distribution of features and the correlation between them at a good level of privacy. Torkezadehmahani et al. [58] introduced a differential privacy condition GAN (CGAN) [59] training framework based on clipping and perturbation strategy, which generates synthetic data and corresponding labels while preserving the privacy of training datasets and uses RDP accountant to track the privacy budget of expenses. Liu et al. [60] proposed a GAN model for privacy protection, which achieves differential privacy by adding carefully designed noise to the clipping gradient in the process of model learning, uses the moment accountant strategy to improve the stability and compatibility of the model by controlling the loss of privacy, and generates high-quality synthetic data while retaining the required available data under a reasonable privacy budget. Ha and Dang [61] proposed a local differential privacy GAN model for noise data generation, which establishes a generative model by clipping the gradient in the model and adding Gaussian noise to the gradient to ensure the differential privacy. Chen et al. [62] proposed gradient-sanitized WGAN, which allows the publication of sanitized sensitive data under strict privacy guarantee and can more accurately distort gradient information so as to train deeper models and generate more information samples. Yang et al. [63] proposed a differential privacy gradient penalty WGAN (WGAN-GP) [64] to train a generative model with privacy protection function, which can provide strong privacy protection for sensitive data and generate high-quality synthetic data. Beaulieu-Jones et al. [65] used the auxiliary classifier GAN (AC-GAN) [66] with differential privacy to generate simulated synthetic participants very similar to Systolic Blood Pressure Trial participants, which can generate synthetic participants and promote secondary analysis and repeatability investigation of clinical datasets by strengthening data sharing and protecting participants' privacy. Fan and Pokkunuru [67] proposed a differential privacy solution for generating high-quality synthetic network flow data, which uses new clipping bound decay and privacy model selection to improve the quality of synthetic data and protects the privacy of sensitive training data by training GAN model with differential privacy. Zhang et al. [68] proposed a privacy publishing model based on GAN for graphs (NetGAN) [69], which can maintain high data utility in degree distribution and satisfy  $(\epsilon, \delta)$ -differential privacy.

Data perturbation can achieve privacy preserving by adding differential privacy noise to training data when using GAN generated synthetic data. Li et al. [70] proposed a graph data privacy protection method using GAN to perform an anonymization operation on graph data, which makes it possible to fully learn the characteristics of graph without specifying specific features and ensures the privacy performance of anonymous graph by adding differential privacy noise to the probability adjacency matrix in the process of graph generation. Neunhoeffler et al. [71] proposed differential privacy post-GAN boosting, which combines the samples produced by the generator sequence obtained during GAN training to create a high-quality synthetic dataset and reweights the generated samples using the private multiplication weight method [72]. Indhumathi and Devi [73] proposed healthcare Cramér GAN, which only adds differential privacy noise to the identified quasi identifiers, and the final result is combined with sensitive attributes, where the anonymous medical data are used as the real data for training Cramér GAN, Cramér distance is used to improve the efficiency of the model, and the synthetic data generation by health care GAN can provide high privacy and overcome various attacks. Imtiaz et al. [74] proposed a GAN combined with differential privacy mechanism to generate a real privacy smart

health care dataset by directly adding noise to the aggregated data record, which can generate high-quality synthetic and differential privacy datasets and retain the statistical characteristics of the original dataset.

**Table 15.** Differential privacy synthetic data generation with GAN.

Existing Work	GAN Type	Clipping Strategy	Perturbation Strategy	Privacy Loss Accountant
[55]	GAN	Clipping gradient	Gradient perturbation	Moment accountant
[56]	WGAN	Clipping weight	Gradient perturbation	Moment accountant
[45]	GAN	Clipping gradient	Gradient perturbation	Moment accountant
[58]	CGAN	Clipping gradient	Gradient perturbation	RDP accountant
[60]	GAN	Clipping gradient	Gradient perturbation	Moment accountant
[61]	GAN	Clipping gradient	Gradient perturbation	Moment accountant
[62]	WGAN	Clipping gradient	Gradient perturbation	RDP accountant
[63]	WGAN-GP	Clipping gradient	Gradient perturbation	Moment accountant
[65]	AC-GAN	Clipping gradient	Gradient perturbation	Moment accountant
[67]	GAN	Clipping gradient	Gradient perturbation	Moment accountant
[68]	NetGAN	Clipping gradient	Gradient perturbation	Privacy budget composition [9]
[70]	GAN	–	Data perturbation	–
[71]	GAN	–	Data perturbation	Advanced composition [9]
[73]	GAN	–	Data perturbation	–
[74]	GAN	–	Data perturbation	–
[75]	GAN	–	Label perturbation	Moment accountant
[76]	GAN	–	Objective function perturbation	Advanced composition
[77]	GAN	–	Differential privacy identifier	Privacy budget composition

By using label perturbation of differential privacy noise, Papernot et al. [78] constructed the private aggregation of teacher ensembles (PATE), which provides a strong privacy guarantee for training data. The mechanism combines multiple models trained by disjoint datasets in a black box way. Because these models rely directly on sensitive data, they are not published but used as “teacher” of the “student” model. Because Laplace noise will only add the output of teachers, the students can learn to predict the output chosen by Laplace noisy voting among all teachers and cannot directly access a single teacher, basic data, or parameters. PATE uses moment accountant to better track privacy costs. Building on the GAN and PATE frameworks, Jordon et al. [75] replaced the GAN discriminator with the PATE mechanism. Therefore, the discriminator satisfies differential privacy, needing a differentiated student version to allow back propagation to the generator. However, this mechanism requires the use of public data.

In objective function perturbation, existing work injects Laplace noise into the coefficients to construct differentially private loss function in GAN training. Zhang et al. [76] proposed a new privacy protection GAN, which perturbs the coefficients of the objective function by injecting Laplace noise into the latent space based on the function mechanism to ensure the differential privacy of the training data, and it is reliable to generate high-quality real synthetic data samples without divulging the sensitive information in the training dataset.

In addition, the current research mainly focuses on publishing privacy-preserving data in a statistical way rather than considering the dynamics and correlation of the context. Thus, on the basis of triple-GAN [79], Ho et al. [77] proposed a generative adversarial game framework with three players based on triple-GAN, which designed a new perceptron,

namely differential privacy identifier, to enhance synthetic data in the way of differential privacy. This deep generative model can generate synthetic data while fulfilling the differential privacy constraint.

### 8.2. Differential Privacy Synthetic Data Generation with Federated Learning

In order to achieve distributed collaborative data analysis, collecting large-scale data is an important task. However, due to the privacy of sensitive data, it is difficult to collect enough samples. Therefore, using GAN can generate synthetic data that can be shared for data analysis. However, in the distributed setting, training GAN faces new challenges of data privacy. Therefore, the existing work provides a solution for differential privacy synthetic data collection by combining GAN and federated learning in a distributed setting. According to the FedAvg training algorithm of model aggregation and averaging, federated learning is achieved by coordinating distributed data with independent and identically distributed and non-IID to perform collaborative learning [80].

Similar to the idea of gradient perturbation, using weight perturbation can achieve differential privacy of a generative model by clipping weight and adding noise to weight in GAN training with federated learning. Machine learning modeler workflow relies on data checking, so it is excluded when direct checking is impossible in the private and decentralized data paradigm. In order to overcome this limitation, Augenstein et al. [81] proposed a differential privacy algorithm, which synthesizes examples representing private data by adding Gaussian noise to the weighted average update.

Gradient perturbation can also be used to ensure the privacy protection of training data in GAN training with federated learning. Chen et al. [62] extended the gradient-sanitized WGAN to train GAN with differential privacy in federated setting and remarked some subtle differences between their method and the method of [81]. Different hospitals jointly train the model through data sharing to diagnose COVID-19 pneumonia, which will also lead to privacy disclosure. In order to solve this problem, Zhang et al. [82] proposed a federated differential privacy GAN for detecting COVID-19 pneumonia, which can effectively diagnose COVID-19 without compromising the privacy under IID and non-IID settings. The distributed storage of data and the fact that data cannot be shared due to privacy reasons for the federated learning environment bringing new challenges to training GAN. Thus, Nguyen et al. [83] proposed a new federated learning scheme to generate realistic COVID-19 images for facilitating enhanced COVID-19 detection with GAN in edge cloud computing, and this scheme integrates a differential privacy solution at each hospital institution to enhance the privacy in federated COVID-19 data analytics. By adding Gaussian noise to the gradient update process of the discriminator, Xin et al. [84] proposed a differential privacy GAN based on federated learning by strategically combining Lipschitz condition and differential privacy sensitivity, which uses a serialized model-training paradigm to significantly reduce the communication cost. Considering that distributed data are often non-IID in reality, which brings challenges to modeling, Xin et al. further proposed universal private FL-GAN to solve this problem. These algorithms can provide strict privacy guarantee using differential privacy, but they can also generate satisfactory data and protect the privacy of training data, even if the data is non-IID.

Furthermore, considering differential average-case privacy [18] enhancing privacy protection of federated learning, Triastcyn and Faltings [85] proposed a privacy protection data publishing framework using GAN in the federated learning environment for which the generator component is trained by the FedAvg algorithm to draw private artificial data samples and empirically evaluate the risk of information disclosure. It can generate high-quality labeled data to successfully train and verify the supervision model, significantly reducing the vulnerability of such models to model inversion attacks.

**Table 16.** Differential privacy synthetic data generation with federated learning.

Existing Work	GAN Type	Clipping Strategy	Perturbation Strategy	Privacy Loss Accountant	Training Method
[81]	GAN	Clipping weight	Weight perturbation	RDP accountant	FedAvg algorithm
[62]	WGAN	Clipping gradient	Gradient perturbation	RDP accountant	FedAvg algorithm
[82]	GAN	Clipping weight	Gradient perturbation	Moment accountant	FedAvg algorithm
[83]	GAN	–	Gradient perturbation	–	FedAvg algorithm
[84]	GAN	Clipping gradient	Gradient perturbation	RDP accountant	Serial training
[85]	GAN	–	Differential average-case privacy	–	FedAvg algorithm

## 9. Open Problems

We survey that the current work focuses on the definitions, privacy-utility metrics, properties, and achieving mechanisms of GDP and LDP based on the information-theoretic channel model. Mir [14] obtained the exponential mechanism achieving GDP by minimizing mutual information on the expected distortion constraint. We can intuitively obtain binary randomized response mechanism, quaternary randomized response mechanism, and multivariate randomized response mechanism under the binary symmetric channel, quasi-symmetric channel, and strongly symmetric channel, respectively, in terms of the Equation (5) of the LDP definition. Wang et al. [38] obtained the  $k$ -subset mechanism by maximizing mutual information about LDP constraint. Although GDP and LDP have been studied based on the information-theoretic channel model, there are some open problems for different application scenarios and data types from the perspective of different types of information-theoretic channel in Table 17.

(1) New LDP from the perspective of information-theoretic channel. Because local users have different privacy preferences, Yang et al. [86] proposed personalized LDP. However, it is necessary to study personalized LDP from the perspective of information-theoretic channel and propose the corresponding achieving mechanism. Although LDP does not require a trusted third party, it regards all local data equally sensitive, which causes excessive protection resulting in utility disaster [87]. Thus, it is necessary to study the utility-optimized mechanism for the setting where all users use the same random perturbation mechanism. In addition, since the differences between sensitive and non-sensitive data vary from user to user, it needs to propose a personalized utility-optimized mechanism of individual data achieving high utility while maintaining privacy preserving of sensitive data. Holohan et al. [42] proposed optimal mechanism satisfying  $(\epsilon, \delta)$ -LDP for randomized response. The optimal mechanism of the randomized response needs to be analyzed and obtained from the perspective of information-theoretic channel. Moreover, a new LDP mechanism needs to be analyzed by using the average error probability [20] as the utility metric under the rate-distortion framework of LDP.

(2) LDP from the perspective of discrete sequence information-theoretic channel. Collecting multiuser high-dimensional data can produce rich knowledge. However, this brings unprecedented privacy concerns to the participants [88,89]. In view of the privacy leakage risk of high-dimensional data aggregation, using the existing LDP mechanism brings poor data utility. Thus, it is necessary to study the optimal LDP mechanism of aggregating high-dimensional data from the perspective of discrete sequence information-theoretic channel. Furthermore, correlations exist between various attributes of high-dimensional data. If the correlation is not modeled, then the high-dimensional correlated data using LDP also leads to poor data utility [90,91]. By constructing the discrete sequence information-theoretic channel model of high-dimensional correlated data aggregation using LDP under joint probability or Markov chain, a LDP mechanism suitable for high-dimensional correlated data aggregation needs to be provided.



**Table 17.** Open problems of GDP and LDP from the perspective of different types of information-theoretic channel.

Scenario	Data Type	Privacy Type	Open Problem	Method	Information-Theoretic Foundation
Data collection	Categorical data	LDP	Personalized privacy demands	Rate-distortion framework	Discrete single symbol information-theoretic channel
			Poor data utility		
			Information-theoretic analysis of existing LDP mechanisms		
High-dimensional (correlated) data collection	Categorical data	LDP	Poor data utility	Rate-distortion framework Joint probability Markov chain	Discrete sequence information-theoretic channel
Continuous (correlated) data releasing	Numerical data	GDP	Information-theoretic analysis of existing GDP mechanisms	Rate-distortion framework Joint probability Markov chain	Continuous information-theoretic channel
			RDP mechanisms		
			Personalized privacy demands		
			Poor data utility		
Multiuser (correlated) data collection	Numerical data	GDP	Privacy leakage risk	Rate-distortion framework	Multiple access channel
	Categorical data	LDP			Multiuser channel with correlated sources
Multi-party data releasing					Broadcast channel
Synthetic data generation	Numerical data	GDP	Poor data utility	GAN	Information-theoretic metrics
	Categorical data	LDP		GAN with federated learning	

(3) GDP from the perspective of continuous information-theoretic channel. For GDP, there is no work to show the direct relationship between GDP mechanisms and single symbol continuous information-theoretic channel model, such as Laplace mechanism, discrete Laplace mechanism, and Gaussian mechanism. RDP is a general privacy definition, but existing work did not provide RDP mechanisms under continuous information-theoretic channel model. Thus, RDP mechanisms need to be studied from the perspective of continuous information-theoretic channel. The continuous releasing of correlated data and their statistics has the potential for significant social benefits. However, privacy concerns hinder the wider use of these continuous correlated data [92,93]. Therefore, the corresponding GDP mechanism from the perspective of continuous multi-symbol information-theoretic channel needs to be studied by combining the joint probability or Markov chain for continuous correlated data releasing with DP. However, it is common that the data curators have different privacy preferences with their data. Thus, personalized DP [94] needs to be studied based on continuous information-theoretic channel model. Existing GDP mechanisms ignore the characteristics of data and directly perturb the data or query results, which will inevitably lead to poor data utility. Therefore, it is necessary to study adaptive GDP depending on characteristics of data [95] from the perspective of continuous information-theoretic channel. Since users have different privacy demands, aggregate data analysis with DP also has poor data utility. Thus, adaptive personalized DP [96] also needs to be studied based on the type of query function, data distribution, and privacy settings from the perspective of continuous information-theoretic channel.

(4) GDP and LDP from the perspective of multiuser information-theoretic channel. A large amount of individual data have aggregated for computing various statistics, query responses, classifiers, and other functions. However, these processes will release sensitive information compromising individual privacy [97–100]. Thus, when considering the aggregation of multiuser data, the GDP and LDP mechanisms need to be studied from the multiple access channel. Data collection of GDP and LDP has been mostly studied for homogeneous and independently distributed data. In real-world applications, data have an inherent correlation which without harnessing will lead to poor data utility [101,102]. Thus, when the multiuser data are correlated, the GDP and LDP mechanisms need to be studied from the perspective of the multiuser channel with correlated sources. With the acceleration of digitization, more and more high-dimensional data are collected and used for different purposes. When these distributed data are aggregated, they can become valuable resources to support better decision making or provide high-quality services. However, because the data held by each party may contain highly sensitive information, simply integrating local data and sharing the aggregation results will pose a serious threat to individual privacy [103,104]. Therefore, GDP and LDP mechanisms need to be studied from the perspective of the broadcast channel for data releasing and sharing of multi-party data.

(5) Adaptive differential privacy with GAN. Existing work can generate differential privacy synthetic data using GAN. However, because of the differential privacy noise introduced in the training, the convergence of GAN becomes even more difficult and leads to the poor utility of output generator at the end of training. Therefore, it is necessary to explore adaptive differential privacy synthetic data using GAN to generate high-quality synthetic data according to the real data distribution. Combining differential privacy definition and information-theoretic metrics, a new differential privacy loss function model of GAN needed to be studied, and the differential privacy loss function model meets the convergence and reaches the optimal solution. Based on differential privacy loss function model, it is needed to construct adaptive differential privacy model. Using GAN and its variants generates synthetic data under adaptive differential privacy model. To improve the quality of the synthetic data using adaptive differential privacy model, GAN modeling is achieved by more layers, more complex structures, or transfer learning. Moreover, speed of GAN training can be accelerated by reducing the privacy budget. To resolve mode collapse and non-convergence issues, it is necessary to conduct fine tuning of hyper parameters, such as learning rate and number of discriminator epochs. Furthermore, the proposed adaptive

differential privacy model with GAN should be extended to a distributed setting by using federated learning, which explores data augmentation methods which can improve the non-IID problem.

## 10. Conclusions

This survey has compared and analyzed the GDP and LDP from the perspective of information-theoretic channel. We concluded that the one-try attack with prior knowledge brings privacy concerns under information-theoretic channel. We described and compared the information-theoretic channel models of GDP and LDP for different data types. We summarized and compared the information-theoretic definitions of GDP and LDP under their information-theoretic channel models and presented the unified information-theoretic definitions of GDP and LDP, respectively. We also made a comparative analysis between GDP (LDP) and other information-theoretic privacy definitions. We surveyed and compared the privacy-utility metrics, properties, and achieving mechanisms of GDP and LDP from the perspective of information-theoretic channel. Moreover, we reviewed the differential privacy synthetic data generation using GAN and GAN with federated learning, respectively. Considering the problem of privacy threat to different real-world applications of different data types, we discussed the open problems from the perspective of different types of information-theoretic channel. We want that the survey can serve as a tutorial for the reader grasping GDP and LDP based on the information-theoretic channel model, and our survey can provide a reference to the reader to conduct in-depth research on GDP and LDP based on different types of information-theoretic channel models.

**Author Contributions:** H.L. wrote the paper and contributed to the review and analysis; H.L., C.P., Y.T., S.L., F.T. and Z.W. collaboratively discussed the results; H.L., C.P., Y.T., S.L., F.T. and Z.W. collaboratively checked the English writing and organization of the manuscript. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported in part by the National Natural Science Foundation of China under Grant 62002081, Grant 62062020, Grant U1836205, and Grant 61602290, in part by the Project Funded by China Postdoctoral Science Foundation under Grant 2019M663907XB, in part by the Natural Science Basic Research Plan in Shaanxi Province of China under Grant 2022JM-329, in part by the Fundamental Research Funds for the Central Universities under Grant GK202103090, in part by the Major Scientific and Technological Special Project of Guizhou Province under Grant 20183001, and in part by the Foundation of Guizhou Provincial Key Laboratory of Public Big Data under Grant 2018BDKFJJ004.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Dwork, C.; McSherry, F.; Nissim, K.; Smith, A. Calibrating noise to sensitivity in private data analysis. In Proceedings of the 3rd Theory of Cryptography Conference, New York, NY, USA, 4–7 March 2006; pp. 265–284.
2. Kasiviswanathan, S.P.; Lee, H.K.; Nissim, K.; Raskhodnikova, S.; Smith, A. What can we learn privately? *SIAM J. Comput.* **2011**, *40*, 793–826. [\[CrossRef\]](#)
3. Liu, H.; Wu, Z.; Peng, C.; Tian, F.; Lu, L. Bounded privacy-utility monotonicity indicating bounded tradeoff of differential privacy mechanisms. *Theor. Comput. Sci.* **2020**, *816*, 195–220. [\[CrossRef\]](#)
4. Dobrota, B. Measuring the Quantity of Data Privacy and Utility Tradeoff for Users' Data: A Visualization Approach. Master Thesis, Utrecht University, Utrecht, The Netherlands, 2021.
5. Kairouz, P.; Oh, S.; Viswanath, P. Extremal mechanisms for local differential privacy. *J. Mach. Learn. Res.* **2016**, *4*, 492–542.
6. Cover, T.M.; Thomas, J.A. *Elements of Information Theory*, 2nd ed.; John Wiley & Sons Inc.: Hoboken, NJ, USA, 2006.
7. Alvim, M.S.; Andrés, M.E.; Chatzikokolakis, K.; Degano, P.; Palamidessi, C. Differential privacy: On the trade-off between utility and information leakage. In Proceedings of the 8th International Workshop on Formal Aspects of Security and Trust, Leuven, Belgium, 12–14 September 2011; pp. 39–54.

8. Barthe, G.; Olmedo, F. Beyond differential privacy: Composition theorems and relational logic for  $f$ -divergences between probabilistic programs. In Proceedings of the 40th International Colloquium Automata, Languages, and Programming, Riga, Latvia, 8–12 July 2013; pp. 49–60.
9. Dwork, C.; Roth, A. The algorithmic foundations of differential privacy. *Found. Trends Theor. Comput. Sci.* **2014**, *9*, 211–407. [[CrossRef](#)]
10. Fehr, S.; Berens, S. On the conditional Rényi entropy. *IEEE Trans. Inf. Theory* **2014**, *60*, 6801–6810. [[CrossRef](#)]
11. Mironov, I. Rényi differential privacy. In Proceedings of the 30th IEEE Computer Security Foundations Symposium, Santa Barbara, CA, USA, 21–25 August 2017; pp. 263–275.
12. Wang, W.; Ying, L.; Zhang, J. On the relation between identifiability, differential privacy, and mutual-information privacy. *IEEE Trans. Inf. Theory* **2016**, *62*, 5018–5029. [[CrossRef](#)]
13. Cuff, P.; Yu, L. Differential privacy as a mutual information constraint. In Proceedings of the 23rd ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 43–54.
14. Mir, D.J. Information-theoretic foundations of differential privacy. In Proceedings of the 5th International Symposium on Foundations and Practice of Security, Montreal, QC, Canada, 25–26 October 2012; pp. 374–381.
15. Smith, G. On the foundations of quantitative information flow. In Proceedings of the 12th International Conference on Foundations of Software Science and Computational Structures, York, UK, 22–29 March 2009; pp. 288–302.
16. Barthe, G.; Köpf, B. Information-theoretic bounds for differentially private mechanisms. In Proceedings of the 24th IEEE Computer Security Foundations Symposium, Cernay-la-Ville, France, 27–29 June 2011; pp. 191–204.
17. Duchi, J.C.; Jordan, M.I.; Wainwright, M.J. Local privacy and statistical minimax rates. In Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science, Berkeley, CA, USA, 26–29 October 2013; pp. 429–438.
18. Duchi, J.C.; Jordan, M.I.; Wainwright, M.J. Privacy aware learning. *J. ACM* **2014**, *61*, 38:1–38:57. [[CrossRef](#)]
19. Jiang, B.; Li, M.; Tandon, R. Context-aware data aggregation with localized information privacy. In Proceedings of the 6th IEEE Conference on Communications and Network Security, Beijing, China, 30 May–1 June 2018; pp. 1–9.
20. Song, H.; Luo, T.; Li, J. Common criterion of privacy metrics and parameters analysis based on error probability for randomized response. *IEEE Access* **2019**, *7*, 16964–16978. [[CrossRef](#)]
21. Lopuhaä-Zwakenberg, M.; Tong, H.; Skoric, B. Data sanitisation protocols for the privacy funnel with differential privacy guarantees. *arXiv* **2020**, arXiv:2008.13151.
22. Lopuhaä-Zwakenberg, M.; Goseling, J. The privacy-utility tradeoff of robust local differential privacy. *arXiv* **2021**, arXiv:2101.09139.
23. Bun, M.; Steinke, T. Concentrated differential privacy: Simplifications, extensions, and lower bounds. In Proceedings of the 14th Theory of Cryptography Conference, Beijing, China, 31 October–3 November 2016; pp. 635–658.
24. Asodeh, S.; Liao, J.; Calmon, F.P.; Kosut, O.; Sankar, L. Three variants of differential privacy: Lossless conversion and applications. *IEEE J. Sel. Areas Inf. Theory* **2021**, *2*, 208–222. [[CrossRef](#)]
25. Chaudhuri, K.; Imola, J.; Machanavajjhala, A. Capacity bounded differential privacy. In Proceedings of the 32nd Annual Conference on Neural Information Processing Systems, Vancouver, BC, Canada, 8–14 December 2019; pp. 3469–3478.
26. Calmon, F.P.; Fawaz, N. Privacy against statistical inference. In Proceedings of the 50th Annual Allerton Conference on Communication, Control, and Computing, Allerton Park & Retreat Center, Monticello, IL, USA, 1–5 October 2012; pp. 1401–1408.
27. Makhdoumi, A.; Fawaz, N. Privacy-utility tradeoff under statistical uncertainty. In Proceedings of the 51st Annual Allerton Conference on Communication, Control, and Computing, Allerton Park & Retreat Center, Monticello, IL, USA, 2–4 October 2013; pp. 1627–1634.
28. Holohan, N.; Leith, D.J.; Mason, O. Extreme points of the local differential privacy polytope. *Linear Algebra Appl.* **2017**, *534*, 78–96. [[CrossRef](#)]
29. De, A. Lower bounds in differential privacy. In Proceedings of the 9th Theory of Cryptography Conference, Taormina, Sicily, Italy, 19–21 March 2012; pp. 321–338.
30. Edwards, T.; Rubinstein, B.I.P.; Zhang, Z.; Zhou, S. A graph symmetrization bound on channel information leakage under Blowfish privacy. *IEEE Trans. Inf. Theory* **2022**, *68*, 538–548. [[CrossRef](#)]
31. Rogers, R.M.; Roth, A.; Smith, A.D.; Thakkar, O. Max-information, differential privacy, and post-selection hypothesis testing. In Proceedings of the 57th Annual Symposium on Foundations of Computer Science, Hyatt Regency, New Brunswick, NJ, USA, 9–11 October 2016; pp. 487–494.
32. Padakandla, A.; Kumar, P.R.; Szpankowski, W. The trade-off between privacy and fidelity via Ehrhart theory. *IEEE Trans. Inf. Theory* **2020**, *66*, 2549–2569. [[CrossRef](#)]
33. Ayed, F.; Battiston, M.; Camerlenghi, F. An information theoretic approach to post randomization methods under differential privacy. *Stat. Comput.* **2020**, *30*, 1347–1361. [[CrossRef](#)]
34. Sarwate, A.D.; Sankar, L. A rate-distortion perspective on local differential privacy. In Proceedings of the 52nd Annual Allerton Conference on Communication, Control, and Computing, Allerton Park & Retreat Center, Monticello, IL, USA, 30 September–3 October 2014; pp. 903–908.
35. Kalantari, K.; Sankar, L.; Sarwate, A.D. Robust privacy-utility tradeoffs under differential privacy and Hamming distortion. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2816–2830. [[CrossRef](#)]

36. Xiong, S.; Sarwate, A.D.; Mandayam, N.B. Randomized requantization with local differential privacy. In Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, Shanghai, China, 20–25 March 2016; pp. 2189–2193.
37. Kalantari, K.; Sankar, L.; Sarwate, A.D. Optimal differential privacy mechanisms under Hamming distortion for structured source classes. In Proceedings of the IEEE International Symposium on Information Theory, Barcelona, Spain, 10–15 July 2016; pp. 2069–2073.
38. Wang, S.; Huang, L.; Nie, Y.; Zhang, X.; Wang, P.; Xu, H.; Yang, W. Local differential private data aggregation for discrete distribution estimation. *IEEE Trans. Parallel Distrib. Syst.* **2019**, *30*, 2046–2059. [[CrossRef](#)]
39. Lopuhaä-Zwakenberg, M.; Skoric, B.; Li, N. Information-theoretic metrics for local differential privacy protocols. *arXiv* **2019**, arXiv:1910.07826.
40. McSherry, F.; Talwar, K. Mechanism design via differential privacy. In Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science, Providence, RI, USA, 20–23 October 2007; pp. 94–103.
41. Duchi, J.C.; Wainwright, M.J.; Jordan, M.I. Local privacy and minimax bounds: Sharp rates for probability estimation. In Proceedings of the 27th Annual Conference on Neural Information Processing Systems, Lake Tahoe, NV, USA, 5–8 December 2013; pp. 1529–1537.
42. Holohan, N.; Leith, D.J.; Mason, O. Optimal differentially private mechanisms for randomised response. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 2726–2735. [[CrossRef](#)]
43. Erlingsson, Ú.; Pihur, V.; Korolova, A. RAPPOR: Randomized aggregatable privacy-preserving ordinal response. In Proceedings of the 21st ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; pp. 1054–1067.
44. Goodfellow, I.J.; Pouget-Abadie, J.; Mirza, M.; Xu, B.; Warde-Farley, D.; Ozair, S.; Courville, A.C.; Bengio, Y. Generative adversarial nets. In Proceedings of the 28th Annual Conference on Neural Information Processing Systems, Montreal, QC, Canada, 8–13 December 2014; pp. 2672–2680.
45. Frigerio, L.; de Oliveira, A.S.; Gomez, L.; Duverger, P. Differentially private generative adversarial networks for time series, continuous, and discrete open data. In Proceedings of the 34th IFIP TC 11 International Conference on ICT Systems Security and Privacy Protection, Lisbon, Portugal, 25–27 June 2019; pp. 151–164.
46. Mukherjee, S.; Xu, Y.; Trivedi, A.; Patowary, N.; Ferres, J.L. privGAN: Protecting GANs from membership inference attacks at low cost to utility. *Proc. Priv. Enhancing Technol.* **2021**, *3*, 142–163. [[CrossRef](#)]
47. Hayes, J.; Melis, L.; Danezis, G.; De Cristofaro, E. LOGAN: Membership inference attacks against generative models. *Proc. Priv. Enhancing Technol.* **2019**, *1*, 133–152. [[CrossRef](#)]
48. Liu, K.S.; Xiao, C.; Li, B.; Gao, J. Performing co-membership attacks against deep generative models. In Proceedings of the 19th IEEE International Conference on Data Mining, Beijing, China, 8–11 November 2019; pp. 459–467.
49. Hilprecht, B.; Härterich, M.; Bernau, D. Monte Carlo and reconstruction membership inference attacks against generative models. *Proc. Priv. Enhancing Technol.* **2019**, *4*, 232–249. [[CrossRef](#)]
50. Chen, D.; Yu, N.; Zhang, Y.; Fritz, M. GAN-leaks: A taxonomy of membership inference attacks against generative models. In Proceedings of the 27th ACM SIGSAC Conference on Computer and Communications Security, Virtual Event USA, 9–13 November 2020; pp. 343–362.
51. Hu, H.; Pang, J. Stealing machine learning models: Attacks and countermeasures for generative adversarial networks. In Proceedings of the 37th Annual Computer Security Applications Conference, Virtual Event USA, 6–10 December 2021; pp. 1–16.
52. Abadi, M.; Chu, A.; Goodfellow, I.J.; McMahan, H.B.; Mironov, I.; Talwar, K.; Zhang, L. Deep learning with differential privacy. In Proceedings of the 23rd ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 308–318.
53. Fan, L. A survey of differentially private generative adversarial networks. In Proceedings of the 1st AAAI Workshop on Privacy-Preserving Artificial Intelligence, New York, NY, USA, 7 February 2020.
54. Cai, Z.; Xiong, Z.; Xu, H.; Wang, P.; Li, W.; Pan, Y. Generative adversarial networks: A survey toward private and secure applications. *ACM Comput. Surv.* **2021**, *54*, 132:1–132:38. [[CrossRef](#)]
55. Lu, P.-H.; Yu, C.-M. POSTER: A unified framework of differentially private synthetic data release with generative adversarial network. In Proceedings of the 24th ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 2547–2549.
56. Xie, L.; Lin, K.; Wang, S.; Wang, F.; Zhou, J. Differentially private generative adversarial network. *arXiv* **2018**, arXiv:1802.06739.
57. Arjovsky, M.; Chintala, S.; Bottou, L. Wasserstein GAN. *arXiv* **2017**, arXiv:1701.07875.
58. Torkzadehmahani, R.; Kairouz, P.; Paten, B. DP-CGAN: Differentially private synthetic data and label generation. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, Long Beach, CA, USA, 16–20 June 2019; pp. 98–104.
59. Mirza, M.; Osindero, S. Conditional generative adversarial nets. *arXiv* **2014**, arXiv:1411.1784.
60. Liu, Y.; Peng, J.; Yu, J.J.Q.; Wu, Y. PPGAN: Privacy-preserving generative adversarial network. In Proceedings of the 25th IEEE International Conference on Parallel and Distributed Systems, Tianjin, China, 4–6 December 2019; pp. 985–989.
61. Ha, T.; Dang, T.K. Investigating local differential privacy and generative adversarial network in collecting data. In Proceedings of the 14th International Conference on Advanced Computing and Applications, Quy Nhon, Vietnam, 25–27 November 2020; pp. 140–145.

62. Chen, D.; Orekondy, T.; Fritz, M. GS-WGAN: A gradient-sanitized approach for learning differentially private generators. In Proceedings of the 34th Annual Conference on Neural Information Processing Systems, virtual, 6–12 December 2020; pp. 12673–12684.
63. Yang, R.; Ma, X.; Bai, X.; Su, X. Differential privacy images protection based on generative adversarial network. In Proceedings of the 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Guangzhou, China, 29 December 2020–1 January 2021; pp. 1688–1695.
64. Gulrajani, I.; Ahmed, F.; Arjovsky, M.; Dumoulin, V.; Courville, A.C. Improved training of Wasserstein GANs. In Proceedings of the 31st Annual Conference on Neural Information Processing Systems, Long Beach, CA, USA, 4–9 December 2017; pp. 5767–5777.
65. Beaulieu-Jones, B.K.; Wu, Z.S.; Williams, C.; Lee, R.; Bhavnani, S.P.; Byrd, J.B.; Greene, C.S. Privacy-preserving generative deep neural networks support clinical data sharing. *Circ. Cardiovasc. Qual.* **2019**, *12*, e005122:1–e005122:10. [[CrossRef](#)]
66. Odena, A.; Olah, C.; Shlens, J. Conditional image synthesis with auxiliary classifier GANs. In Proceedings of the 34th International Conference on Machine Learning, Sydney, NSW, Australia, 6–11 August 2017; pp. 2642–2651.
67. Fan, L.; Pokkunuru, A. DPNeT: Differentially private network traffic synthesis with generative adversarial networks. In Proceedings of the 35th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy, Calgary, AB, Canada, 19–20 July 2021; pp. 3–21.
68. Zhang, S.; Ni, W.; Fu, N. Differentially private graph publishing with degree distribution preservation. *Comput. Secur.* **2021**, *106*, 102285:1–102285:17. [[CrossRef](#)]
69. Bojchevski, A.; Shchur, O.; Zügner, D.; Günnemann, S. NetGAN: Generating graphs via random walks. In Proceedings of the 35th International Conference on Machine Learning, Stockholmsmässan, Stockholm, Sweden, 10–15 July 2018; pp. 609–618.
70. Li, A.; Fang, J.; Jiang, Q.; Zhou, B.; Jia, Y. A graph data privacy-preserving method based on generative adversarial networks. In Proceedings of the 21st International Conference on Web Information Systems Engineering, Amsterdam, The Netherlands, 20–24 October 2020; pp. 227–239.
71. Neunhoffer, M.; Wu, S.; Dwork, C. Private post-GAN boosting. In Proceedings of the 9th International Conference on Learning Representations, Virtual Event Austria, 3–7 May 2021.
72. Hardt, M.; Rothblum, G.N. A multiplicative weights mechanism for privacy-preserving data analysis. In Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science, Las Vegas, NV, USA, 23–26 October 2010; pp. 61–70.
73. Indhumathi, R.; Devi, S.S. Healthcare Cramér generative adversarial network (HCGAN). *Distrib. Parallel. Dat.* **2021**, *39*, 1–17. [[CrossRef](#)]
74. Imtiaz, S.; Arsalan, M.; Vlassov, V.; Sadre, R. Synthetic and private smart health care data generation using GANs. In Proceedings of the 30th International Conference on Computer Communications and Networks, Athens, Greece, 19–22 July 2021; pp. 1–7.
75. Jordon, J.; Yoon, J.; van der Schaar, M. PATE-GAN: Generating synthetic data with differential privacy guarantees. In Proceedings of the 7th International Conference on Learning Representations, New Orleans, LA, USA, 6–9 May 2019.
76. Zhang, X.; Ding, J.; Errapotu, S.M.; Huang, X.; Li, P.; Pan, M. Differentially private functional mechanism for generative adversarial networks. In Proceedings of the IEEE Global Communications Conference, GLOBECOM 2019, Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.
77. Ho, S.; Qu, Y.; Gu, B.; Gao, L.; Li, J.; Xiangy, Y. DP-GAN: Differentially private consecutive data publishing using generative adversarial nets. *J. Netw. Comput. Appl.* **2021**, *185*, 103066:1–103066:11. [[CrossRef](#)]
78. Papernot, N.; Abadi, M.; Erlingsson, Ú.; Goodfellow, I.J.; Talwar, K. Semi-supervised knowledge transfer for deep learning from private training data. In Proceedings of the 5th International Conference on Learning Representations, Toulon, France, 24–26 April 2017.
79. Li, C.; Xu, T.; Zhu, J.; Zhang, B. Triple generative adversarial nets. In Proceedings of the 31st Annual Conference on Neural Information Processing Systems, Long Beach, CA, USA, 4–9 December 2017; pp. 4088–4098.
80. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; Arcas, B.A. Communication-efficient learning of deep networks from decentralized data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, Fort Lauderdale, FL, USA, 20–22 April 2017; pp. 1273–1282.
81. Augenstein, S.; McMahan, H.B.; Ramage, D.; Ramaswamy, S.; Kairouz, P.; Chen, M.; Mathews, R.; Arcas, B.A. Generative models for effective ml on private, decentralized datasets. In Proceedings of the 8th International Conference on Learning Representations, Addis Ababa, Ethiopia, 26–30 April 2020.
82. Zhang, L.; Shen, B.; Barnawi, A.; Xi, S.; Kumar, N.; Wu, Y. FedDPGAN: Federated differentially private generative adversarial networks framework for the detection of COVID-19 pneumonia. *Inf. Syst. Frontiers* **2021**, *23*, 1403–1415. [[CrossRef](#)] [[PubMed](#)]
83. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Zomaya, A.Y. Federated learning for COVID-19 detection with generative adversarial networks in edge cloud computing. *IEEE Internet Things* **2021**. [[CrossRef](#)]
84. Xin, B.; Geng, Y.; Hu, T.; Chen, S.; Yang, W.; Wang, S.; Huang, L. Federated synthetic data generation with differential privacy. *Neurocomputing* **2022**, *468*, 1–10. [[CrossRef](#)]
85. Triastcyn, A.; Faltings, B. Federated generative privacy. *IEEE Intell. Syst.* **2020**, *35*, 50–57. [[CrossRef](#)]
86. Yang, G.; Wang, S.; Wang, H. Federated learning with personalized local differential privacy. In Proceedings of the 6th IEEE International Conference on Computer and Communication Systems, Chengdu, China, 23–26 April 2021; pp. 484–489.
87. Murakami, T.; Kawamoto, Y. Utility-optimized local differential privacy mechanisms for distribution estimation. In Proceedings of the 28th USENIX Security Symposium, Santa Clara, CA, USA, 14–16 August 2019; pp. 1877–1894.

88. Ren, X.; Yu, C.-M.; Yu, W.; Yang, S.; Yang, X.; McCann, J.A.; Yu, P.S. LoPub: High-dimensional crowdsourced data publication with local differential privacy. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2151–2166. [[CrossRef](#)]
89. Wang, N.; Xiao, X.; Yang, Y.; Zhao, J.; Hui, S.C.; Shin, H.; Shin, J.; Yu, G. Collecting and analyzing multidimensional data with local differential privacy. In Proceedings of the 35th IEEE International Conference on Data Engineering, Macao, China, 8–11 April 2019; pp. 638–649.
90. Ren, X.; Xu, J.; Yang, X.; Yang, S. Bayesian network-based high-dimensional crowdsourced data publication with local differential privacy. *Sci. Sin. Inform.* **2019**, *49*, 1586–1605.
91. Du, R.; Ye, Q.; Fu, Y.; Hu, H. Collecting high-dimensional and correlation-constrained data with local differential privacy. In Proceedings of the 18th Annual IEEE International Conference on Sensing, Communication, and Networking, Rome, Italy, 6–9 July 2021; pp. 1–9.
92. Hemkumar, D.; Ravichandra, S.; Somayajulu, D.V.L.N. Impact of data correlation on privacy budget allocation in continuous publication of location statistics. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 1650–1665. [[CrossRef](#)]
93. Cao, Y.; Yoshikawa, M.; Xiao, Y.; Xiong, L. Quantifying differential privacy in continuous data release under temporal correlations. *IEEE Trans. Knowl. Data Eng.* **2019**, *31*, 1281–1295. [[CrossRef](#)]
94. Jorgensen, Z.; Yu, T.; Cormode, G. Conservative or liberal? Personalized differential privacy. In Proceedings of the 31st IEEE International Conference on Data Engineering, Seoul, Korea, 13–17 April 2015; pp. 1023–1034.
95. Chen, Y.; Machanavajjhala, A.; Hay, M.; Miklau, G. PeGaSus: Data-adaptive differentially private stream processing. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 1375–1388.
96. Niu, B.; Chen, Y.; Wang, B.; Wang, Z.; Li, F.; Cao, J. AdaPDP: Adaptive personalized differential privacy. In Proceedings of the 40th IEEE Conference on Computer Communications, Vancouver, BC, Canada, 10–13 May 2021; pp. 1–10.
97. Pathak, M.A.; Rane, S.; Raj, B. Multiparty differential privacy via aggregation of locally trained classifiers. In Proceedings of the 24th Annual Conference on Neural Information Processing Systems, Vancouver, BC, Canada, 6–9 December 2010; pp. 1876–1884.
98. Wei, K.; Li, J.; Ding, M.; Ma, C.; Yang, H.H.; Farokhi, F.; Jin, S.; Quek, T.Q.S.; Poor, H.V. Federated learning with differential privacy: Algorithms and performance analysis. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3454–3469. [[CrossRef](#)]
99. Sun, L.; Qian, J.; Chen, X. LDP-FL: Practical private aggregation in federated learning with local differential privacy. In Proceedings of the 30th International Joint Conference on Artificial Intelligence, Montréal, QC, Canada, 19–20 August 2021; pp. 1571–1578.
100. Wu, S.; Yu, M.; Ahmed, M.A.M.; Qian, Y.; Tao, Y. FL-MAC-RDP: Federated learning over multiple access channels with renyi differential privacy. *Int. J. Theor. Phys.* **2021**, *60*, 2668–2682. [[CrossRef](#)]
101. Niu, C.; Zheng, Z.; Wu, F.; Tang, S.; Gao, X.; Chen, G. Unlocking the value of privacy: Trading aggregate statistics over private correlated data. In Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, London, UK, 19–23 August 2018; pp. 2031–2040.
102. Gu, X.; Li, M.; Cheng, Y.; Xiong, L.; Cao, Y. PCKV: Locally differentially private correlated key-value data collection with optimized utility. In Proceedings of the 29th USENIX Security Symposium, Boston, MA, USA, 12–14 August 2020; pp. 967–984.
103. Cheng, X.; Tang, P.; Su, S.; Chen, R.; Wu, Z.; Zhu, B. Multi-party high-dimensional data publishing under differential privacy. *IEEE Trans. Knowl. Data Eng.* **2020**, *32*, 1557–1571. [[CrossRef](#)]
104. Zheng, X.; Cai, Z. Privacy-preserved data sharing towards multiple parties in industrial IoTs. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 968–979. [[CrossRef](#)]