

# A Survey of Local Differential Privacy and Its Variants

Likun Qin, Nan Wang, Tianshuo Qiu

Department of Electrical and Computer Engineering

Shandong University, Jinan, China

**Abstract**—The introduction and advancements in Local Differential Privacy (LDP) variants have become a cornerstone in addressing the privacy concerns associated with the vast data produced by smart devices, which forms the foundation for data-driven decision-making in crowdsensing. While harnessing the power of these immense data sets can offer valuable insights, it simultaneously poses significant privacy risks for the users involved. LDP, a distinguished privacy model with a decentralized architecture, stands out for its capability to offer robust privacy assurances for individual users during data collection and analysis. The essence of LDP is its method of locally perturbing each user's data on the client-side before transmission to the server-side, safeguarding against potential privacy breaches at both ends. This article offers an in-depth exploration of LDP, emphasizing its models, its myriad variants, and the foundational structure of LDP algorithms.

## I. INTRODUCTION

Collecting and analyzing data introduces significant privacy concerns because it often includes sensitive user information. With the advent of sophisticated data fusion and analysis methods, user data becomes even more susceptible to breaches and exposure in this era of big data. For instance, by studying appliance usage, adversaries can deduce daily routines or behaviors of individuals, like when they are home or their specific activities such as watching TV or cooking. It's crucial to prioritize the protection of personal data when gathering information from diverse devices. Currently, the European Union (EU) has released the GDPR [1], which oversees EU data protection laws for its citizens and outlines the specifics related to the handling of personal data. Similarly, the U.S. National Institute of Standards and Technology (NIST) is in the process of crafting privacy frameworks. These frameworks aim to more effectively recognize, evaluate, and address privacy risks, enabling individuals to embrace innovative technologies with increased trust and confidence [2], [3].

From a privacy-protection standpoint, differential privacy (DP) has been introduced over a decade ago [4], [5]. Recognized as a robust framework for safeguarding privacy, it's often termed as global DP or centralized DP. DP's strength lies in its mathematical rigor; it operates independent of an adversary's background knowledge and assures potent privacy protection for users. It has found applications across various domains [6]. However, DP assumes the presence of a trustworthy server, which can be a challenge since many online platforms or crowdsourcing systems might have untrustworthy servers keen on user data statistics [7], [8].

Emerging from the concept of DP, local differential privacy (LDP) was introduced [9]. LDP stands as a decentralized version of DP, offering individualized privacy assurances and making no assumptions about third-party server trustworthiness. LDP has become a focal point in privacy research due to its theoretical significance and practical implications [10]. Numerous corporations, including Apple's iOS [11], Google Chrome, and the Windows operating system, have integrated LDP-driven algorithms into their systems. Owing to its robust capabilities, LDP has become a preferred choice to address individual privacy concerns during various statistical and analytical operations. This includes tasks like frequency and mean value estimation [12], the identification of heavy hitters [13], k-way marginal release, empirical risk minimization (ERM), federated learning, and deep learning.

While LDP is powerful, it's not without its challenges, notably in striking an optimal balance between utility and privacy [14]. To address this, there are two primary approaches. Firstly, by devising improved mechanisms - leading to the introduction of numerous LDP-based protocols and sophisticated mechanisms in academic circles. Secondly, by revisiting the definition of LDP itself, with researchers suggesting more flexible privacy concepts to better cater to the utility-privacy balance required for real-world applications. Given the growing significance of LDP, a thorough survey of the topic is both timely and essential. While there exists some literature reviewing LDP, the focus has often been narrow. They either focus on specific applications or certain types of mechanisms.

In this paper, we delve deep into the world of LDP and its various offshoots, meticulously studying their recent advancements and associated mechanisms. We embark on a thorough exploration of the foundational principles that drive LDP and the evolutionary trajectories of its multiple variants. We aim to identify the cutting-edge developments, shedding light on the innovations that have shaped these privacy tools and the challenges they aim to address in our contemporary digital landscape. Furthermore, we analyze the specific mechanisms that support and enhance the capabilities of LDP, understanding their technical intricacies and the real-world applications they cater to. Through this comprehensive study, we aspire to provide readers with a panoramic view of the current state of LDP research, setting the stage for future inquiries and innovations in this critical domain.

## II. LOCAL DIFFERENTIAL PRIVACY, PROPERTIES AND MECHANISMS

In this section, we study LDP and its properties, and LDP based mechanisms. We start from the definition of LDP.

**Definition 1** ( $\varepsilon$ -Local Differential Privacy ( $\varepsilon$ -LDP) .

A randomized mechanism  $M$  satisfies  $\varepsilon$ -LDP if and only if for any pairs of input values  $v, v'$  in the domain of  $M$ , and for any possible output  $y \in Y$ , it holds

$$P[M(v) = y] \leq e^\varepsilon \cdot P[M(v') = y], \quad (1)$$

where  $P[\cdot]$  denotes probability and  $\varepsilon$  is the privacy budget. A smaller  $\varepsilon$  means stronger privacy protection, and vice versa.

The basic properties of LDP include the followings:

**Composition:** [15] Given two mechanisms  $M_1$  and  $M_2$  that provide  $\varepsilon_1$ -LDP and  $\varepsilon_2$ -LDP respectively, their sequential composition provides  $(\varepsilon_1 + \varepsilon_2)$ -LDP.

$$M(v) = (M_1(v), M_2(v)) \implies M \text{ is } (\varepsilon_1 + \varepsilon_2)\text{-LDP} \quad (2)$$

**Post-processing:** Any function applied to the output of an  $\varepsilon$ -LDP mechanism retains the  $\varepsilon$ -LDP guarantee.

$$\text{If } M(v) \text{ is } \varepsilon\text{-LDP, then } f(M(v)) \text{ is also } \varepsilon\text{-LDP.} \quad (3)$$

**Robustness to Side Information:** LDP guarantees hold even if an adversary has access to auxiliary or side information.

**Utility-Privacy Tradeoff:** Generally, a lower value of  $\varepsilon$  implies stronger privacy but might result in reduced utility of the perturbed data.

**Independence of Background Knowledge:** The privacy guarantees of LDP mechanisms are designed to hold regardless of any background knowledge an adversary might have.

Next, we study mechanisms that satisfy LDP:

**Randomize Response** [16]

The Randomized Response Mechanism is a simple yet effective approach to achieving LDP. It's particularly used for binary data, i.e., when a user's data item is either 0 or 1. The mechanism operates as follows:

- 1) With probability  $\frac{1}{2}$ , the user truthfully answers a question.
- 2) With probability  $\frac{1}{2}$ , the user randomly answers the question.

Mathematically, given a user's true data item  $v \in \{0, 1\}$ , the mechanism outputs  $v$  with probability  $\frac{1}{2}$  and outputs  $1 - v$  (i.e., the opposite of  $v$ ) with probability  $\frac{1}{2}$ .

The probability mass function (pmf) is given by:

$$P[M(v) = 1] = \frac{1}{2}v + \frac{1}{2}(1 - v) = \frac{1}{2} \quad (4)$$

$$P[M(v) = 0] = \frac{1}{2}(1 - v) + \frac{1}{2}v = \frac{1}{2} \quad (5)$$

This mechanism ensures  $\varepsilon$ -LDP with  $\varepsilon = \ln(2)$ .

**Laplace Mechanism** [17]

The Laplace Mechanism adds noise drawn from the Laplace distribution to the true value of the data. For LDP, this mechanism can be adjusted as:

Given a data item  $v$ , the mechanism outputs:

$$M(v) = v + \text{Lap}\left(\frac{\Delta f}{\varepsilon}\right)$$

where  $\Delta f$  is the sensitivity of the function  $f$  and  $\text{Lap}(\cdot)$  represents the Laplace distribution.

**Gaussian Mechanism**

Similar to the Laplace Mechanism, the Gaussian Mechanism adds noise but from the Gaussian distribution:

Given a data item  $v$ , the mechanism outputs:

$$M(v) = v + \mathcal{N}(0, \sigma^2)$$

where  $\sigma^2$  determines the amount of noise based on the desired  $\varepsilon$  and function sensitivity  $\Delta f$ .

**Exponential Mechanism**

The Exponential Mechanism selects an output based on a scoring function and weights outputs with the exponential of their score. Given a set of possible outputs  $R$ , a data item  $v$ , and a scoring function  $q(v, r)$ , the probability of selecting output  $r$  is proportional to:

$$\exp\left(\frac{\varepsilon q(v, r)}{2\Delta q}\right)$$

where  $\Delta q$  is the sensitivity of  $q$ .

**Perturbed Histogram Mechanism**

For a set of items, instead of perturbing each item, this mechanism perturbs the histogram of the data items. Given a data item set  $V$ , the mechanism constructs a histogram  $H$  and then outputs:

$$M(H) = H + \text{Lap}\left(\frac{\Delta H}{\varepsilon}\right)$$

where  $\Delta H$  is the sensitivity of the histogram construction.

Observe that each mechanism's efficacy is closely tied to the sensitivity of the query, denoted as  $\Delta f$ . In the realm of Local Differential Privacy (LDP), this sensitivity can often grow significantly, especially when the input domain is vast. The larger the sensitivity, the more noise needs to be introduced by the mechanism to ensure the desired privacy level. This can lead to significant distortion in the data, compromising its utility.

Furthermore, as the input support size increases, maintaining the desired privacy guarantee becomes a challenge. Noise calibrated to a high sensitivity can sometimes overshadow the actual data, rendering the results almost meaningless or leading to misinterpretations.

The consequence of this is a pronounced tradeoff between utility and privacy. Achieving stronger privacy often means accepting reduced accuracy and utility in the results, and vice versa. For applications that require high precision, this can be problematic. It implies that while these mechanisms provide a robust privacy guarantee in theory, their practical applicability can be constrained, especially in scenarios where fine-grained insights from data are crucial.

Hence, while the promise of LDP is enticing, its real-world implementation requires careful consideration of the utility-privacy balance, pushing researchers to seek more efficient mechanisms or modified privacy models to better cater to practical needs.

### III. ADVANCED LDP MECHANISMS

As we mentioned in the introduction, to improve the utility-privacy tradeoff provided by LDP, there are typically two manners. One is to design dedicated mechanism or advanced protocols. The other is to relax the definition of LDP to enhance the data utility. In this section, we summarized several advanced LDP algorithms, aiming to improve the general utility-privacy tradeoff.

#### RAPPOR [10] (Randomized Aggregatable Privacy-Preserving Ordinal Response):

Introduced by Google. RAPPOR enhances the randomized response mechanism through the incorporation of Bloom filters. Each user's value is hashed multiple times into a Bloom filter, which is then perturbed using the RR technique. This allows multiple string values to be encoded before randomization. Advantage: Its main strength lies in collecting statistics about low-frequency items in the user population. It can provide meaningful insights even when items are not commonly observed.

#### Local Hashing [12]:

Addressing the problem of efficiency in the RR technique when dealing with a large domain of inputs, local hashing maps the original vast domain into a smaller domain using hash functions. This condensed domain can then be analyzed using traditional RR techniques. Advantage: It substantially reduces the noise introduced in the randomization process, enabling accurate estimation of frequencies for individual items in the domain. This mechanism improves the utility, especially when the original domain is considerably large.

#### Piecewise RR:

Instead of applying the same randomization mechanism across the entire input domain, the Piecewise RR technique divides the domain into multiple segments or pieces. Each segment then gets its own randomization mechanism tailored to its characteristics. Advantage: This method achieves a more granular utility-privacy tradeoff. It can offer enhanced privacy in sensitive segments while improving utility in less-sensitive ones. Optimized RR:

The protocol doesn't just use a fixed randomization parameter; instead, it optimizes the parameters of the RR. This optimization is often based on real data distribution or some auxiliary information, ensuring that the randomization provides the best possible utility. Advantage: By adjusting the randomization according to data distribution, it achieves better accuracy in aggregate statistics.

#### Fourier Perturbation Algorithm (FPA) [18]:

Instead of perturbing the raw data directly, FPA operates in the frequency domain. The data undergoes a Fourier transformation, after which the perturbation is applied. This allows for randomization in a different space that might be more conducive to certain types of analyses. Advantage: Provides enhanced utility for specific query types, especially those that are frequency-based or need insights from periodic patterns in data.

### IV. LDP VARIANTS AND MECHANISMS

In this section, we introduce LDP variants that aim to provide better utility-privacy tradeoff in different applications.

#### A. Variants and Mechanisms of LDP

1)  $(\varepsilon, \delta)$ -LDP: Drawing parallels with how  $(\varepsilon, \delta)$ -DP [19] extends  $\varepsilon$ -DP,  $(\varepsilon, \delta)$ -LDP (sometimes termed as approximate LDP) serves as a more flexible counterpart to  $\varepsilon$ -LDP (or pure LDP).

**Definition 1** (Approximate Local Differential Privacy). A randomized process  $M$  complies with  $(\varepsilon, \delta)$ -LDP if, for all input pairs  $v$  and  $v'$  within  $M$ 's domain and any probable output  $y \in Y$ , the following holds:

$$P[M(v) = y] \leq e^\varepsilon \cdot P[M(v') = y] + \delta.$$

Here,  $\delta$  is customarily a small value.

In essence,  $(\varepsilon, \delta)$ -LDP implies that  $M$  achieves  $\varepsilon$ -LDP with a likelihood not less than  $1 - \delta$ . If  $\delta = 0$ ,  $(\varepsilon, \delta)$ -LDP converges to  $\varepsilon$ -LDP.

2) BLENDER Model: BLENDER [20], a fusion of global DP and LDP, optimizes data utility while retaining privacy. It classifies users based on their trust in the aggregator into two categories: the opt-in group and clients. BLENDER enhances utility by balancing data from both. Its privacy measure mirrors that of  $(\varepsilon, \delta)$ -DP [21].

3) Geo-indistinguishability: Originally tailored for location privacy with global DP, Geo-indistinguishability [22] uses the data's geographical distance. Alvim et al. [23] argued for metric-based LDP's advantages in specific contexts.

**Definition 2** (Geo-indistinguishability). A randomized function  $M$  adheres to Geo-indistinguishability if, for any input pairs  $v$  and  $v'$  and any output  $y \in Y$ , the subsequent relation is met:

$$P[M(v) = y] \leq e^{\varepsilon \cdot d(v, v')} \cdot P[M(v') = y],$$

where  $d(., .)$  designates a distance metric.

This model adjusts privacy depending on data distance, augmenting utility for datasets like location or smart meter consumption that are sensitive to distance.

4) Local Information Privacy: Local Information Privacy (LIP) was originally proposed in [24] as a prior-aware version of LDP, and then, in [25], Jiang et al relax the prior-aware assumption to partial prior-aware (Bounded Prior in their version). The definition of LIP is shown as follows:

**Definition 3.**  $(\varepsilon, \delta)$ -Local Information Privacy [26] A mechanism  $M$  satisfies  $(\varepsilon, \delta)$ -LIP, if  $\forall x \in \mathcal{X}$ ,  $y \in Range(\mathcal{M})$ :

$$\begin{aligned} P(Y = y) &\geq e^{-\varepsilon} P(Y = y | X = x) - \delta, \\ P(Y = y) &\leq e^\varepsilon P(Y = y | X = x) + \delta. \end{aligned} \quad (6)$$

5) Sequential Information Privacy: Sequential Information Privacy (SIP), built upon LIP, measures the privacy leakage for a data sequence, or time series data. SIP naturally decomposes using chain rule-similar techniques and is comparable to that of LDP.

**Definition 4.** [ $(\epsilon)$ -Sequence Information Privacy] [27] A mechanism  $\mathcal{M}$  satisfies  $(\epsilon)$ -SIP for some  $\epsilon \in \mathbb{R}^+$ , if  $\forall X_1^T \in \mathcal{X}$ ,  $Y_1^T \in Range(\mathcal{M})$ :

$$e^{-\epsilon} \leq \frac{P[M(x_1^T) = y_1^T]}{P[X_1^T = x_1^T]} \leq e^\epsilon \quad (7)$$

The operational meaning of LIP is, the output  $Y$  provides limited additional information about any possible input  $X$ , and the amount of the additional information is measured by the privacy budget  $\epsilon$  and failure probability  $\delta$ .

In [28], multiple LIP mechanisms were proposed and testified, showing that even though  $\epsilon$ -LIP is stronger than  $2\epsilon$ -LDP in terms of privacy protection. The mechanisms achieve more than 2 times of utility gain.

6) *CLDP*: Recognizing LDP's diminished utility with fewer users, Gursoy et al. [29] introduced the metric-based model of condensed local differential privacy (CLDP).

**Definition 5** ( $\alpha$ -CLDP). *For all input pairs  $v$  and  $v'$  in  $M$ 's domain and any potential output  $y \in Y$ , a randomized function  $M$  satisfies  $\alpha$ -CLDP if:*

$$P[M(v) = y] \leq e^{\alpha \cdot d(v, v')} \cdot P[M(v') = y],$$

where  $\alpha > 0$ .

In CLDP, a decline in  $\alpha$  compensates for a growth in distance  $d$ . Gursoy et al. employed an Exponential Mechanism variant to devise protocols, particularly benefitting scenarios with limited users.

7) *PLDP*: PLDP [30] offers user-specific privacy levels. Here, users can modify their privacy settings, denoted by  $\varepsilon$ .

**Definition 6** ( $\varepsilon$ -PLDP). *For a user  $U$ , and all input pairs  $v$  and  $v'$  in  $M$ 's domain and any potential output  $y \in Y$ , a randomized function  $M$  meets  $\varepsilon_U$ -PLDP if:*

$$P[M(v) = y] \leq e^{\varepsilon_U} \cdot P[M(v') = y].$$

Approaches like the personalized count estimation protocol and advanced combination strategy cater to users with varying privacy inclinations.

8) *Utility-optimized LDP (ULDP)*: Traditional LDP assumes all data points have uniform sensitivity, often causing excessive noise addition. Recognizing that not all personal data have equivalent sensitivity, the Utility-optimized LDP (ULDP) model was proposed. In this model, let  $KS \subseteq K$  be the sensitive dataset and  $KN = K \setminus KS$  be the non-sensitive dataset. Let  $Y_P \subseteq Y$  be the protected output set and  $Y_I = Y \setminus Y_P$  be the invertible output set. The formal definition of ULDP is:

**Definition 7.** *Given  $KS \subseteq K$ ,  $Y_P \subseteq Y$ , a mechanism  $M$  adheres to  $(KS, Y_P, \epsilon)$ -ULDP if:*

- For every  $y \in Y_I$ , there is a  $v \in KN$  with  $P[M(v) = y] > 0$  and  $P[M(v') = y] = 0$  for any  $v' \neq v$ .
- For all  $v, v' \in K$  and  $y \in Y_P$ ,  $P[M(v) = y] \leq e^\epsilon \cdot P[M(v') = y]$ .

In simpler terms,  $(KS, Y_P, \epsilon)$ -ULDP ensures that sensitive inputs are mapped only to the protected output set.

9) *Input-Discriminative LDP (ID-LDP)*: While ULDP classifies data as either sensitive or non-sensitive, the ID-LDP model offers a more nuanced approach by acknowledging varying sensitivity levels among data. It is defined as:

**Definition 8.** *Given a set of privacy budgets  $E = \{\epsilon_v\}_{v \in K}$ , a mechanism  $M$  adheres to E-ID-LDP if for all input pairs  $v$  and  $v'$ , and any output  $y \in Y$ :*

$$P[M(v) = y] \leq e^{r(\epsilon_v, \epsilon_{v'})} \cdot P[M(v') = y]$$

where  $r(\cdot, \cdot)$  is a function of two privacy budgets.

The study in [31] primarily utilizes the minimum function between  $\epsilon_v$  and  $\epsilon_{v'}$  and introduces the MinID-LDP as a specialized case.

10) *Parameter Blending Privacy (PBP)*: PBP was proposed as a more flexible LDP variant [32]. In PBP, let  $\Theta$  represent the domain of privacy parameters. Given a privacy budget  $\theta \in \Theta$ , let  $P(\theta)$  denote the frequency with which  $\theta$  is selected. PBP is defined as:

**Definition 9.** *A mechanism  $M$  adheres to r-PBP if, for all  $\theta \in \Theta$ ,  $v, v' \in K$ ,  $y \in Y$ , there exists a  $\theta' \in \Theta$  such that:*

$$P(\theta)P[M(v; \theta) = y] \leq e^{r(\theta)} \cdot P(\theta')P[M(v'; \theta') = y]$$

## B. A Summary of LDP variants

Local Differential Privacy (LDP) is a foundational approach tailored for all data types and operates using the randomized response (RR) technique. Its primary advantage is its broad applicability, but it may add more noise than necessary, especially when not all data attributes have the same sensitivity levels. To address this, approximate LDP, which allows for minor violations in privacy guarantees, introduces flexibility. However, this relaxation can be a double-edged sword, potentially compromising privacy in highly sensitive scenarios.

BLENDER, on the other hand, is crafted explicitly for categorical data. By synergizing aspects of both global Differential Privacy and LDP, it aims to improve data utility. Yet, its reliance on grouping user data might introduce challenges in dynamic or constantly changing environments. Local d-privacy is another variant, designed with metric spaces in mind. It's particularly beneficial for data like location points, but may not be the first choice for other data structures due to its specific metric-based method.

CLDP stands out for its unique approach to address challenges that arise with smaller user counts, an often overlooked but crucial aspect in privacy. However, while it addresses issues in smaller datasets, it might introduce complexities when the user base grows, making scalability a potential concern. PLDP, meanwhile, strives to provide a more granular level of privacy. While this granularity is its strength, the trade-off might be a more significant computational overhead and intricate implementation details.

ULDP takes a novel stance by focusing on optimizing utility through an emphasis on sensitive data. The premise here is that not all data pieces hold equal sensitivity. However, the challenge and responsibility of correctly categorizing which data is sensitive can be daunting. ID-LDP further refines this concept by providing protection based on the actual sensitivity of the input, using unary encoding to achieve this. Its main challenge is the intricate parameter setting required to ensure optimal performance. Lastly, PBP is distinct in its pursuit of robust privacy. By maintaining the secrecy of provider

parameters, it bolsters privacy assurances. Yet, this added layer of secrecy might introduce complexities in implementation and understanding.

## V. CONCLUSION

In the realm of data privacy, Local Differential Privacy (LDP) stands out as a vital tool for preserving user data. This research delves into various LDP mechanisms, protocols and variants in definition, each addressing unique challenges. From the foundational LDP to specialized versions like BLENDER for categorical data and Local d-privacy for metrics, the spectrum of solutions is vast. Techniques like CLDP tackle smaller datasets, while PLDP, ULDP, and ID-LDP optimize data utility and privacy levels. The introduction of PBP emphasizes secrecy in privacy parameters. Ultimately, this paper underscores the importance of selecting the right LDP variant, given the specific nature of data and privacy needs.

## REFERENCES

- [1] European Parliament and Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council. [Online]. Available: <https://data.europa.eu/eli/reg/2016/679/oj>
- [2] R. MEYER. (2014) Facebook's mood manipulation experiment might have been illegal. [Online]. Available: <https://www.theatlantic.com/technology/archive/2014/09/facebook-mood-manipulation/374484/>
- [3] "No free lunch in data privacy," in *Proceedings of SIGMOD 2011 and PODS 2011*, ser. Proceedings of the ACM SIGMOD International Conference on Management of Data. Association for Computing Machinery, 2011, pp. 193–204.
- [4] C. Dwork, F. McSherry, and K. Nissim, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography: Third Theory of Cryptography Conference*, 2006, pp. 265–284. [Online]. Available: [https://doi.org/10.1007/11681878\\_14](https://doi.org/10.1007/11681878_14)
- [5] C. Dwork, "Differential privacy," in *Automata, Languages and Programming: 33rd International Colloquium, ICALP 2006, Part II*, M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, Eds., 2006, pp. 1–12. [Online]. Available: [https://doi.org/10.1007/11787006\\_1](https://doi.org/10.1007/11787006_1)
- [6] Y. Xiao and L. Xiong, "Protecting locations with differential privacy under temporal correlations," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '15, New York, NY, USA, 2015, p. 1298–1309.
- [7] W. Primoff and S. Kess, "The equifax data breach: What cpas and firms need to know now," *The CPA Journal*, vol. 87, no. 12, pp. 14–17, 2017.
- [8] J. Lu, "Assessing the cost, legal fallout of capital one data breach," *Legal Fallout Of Capital One Data Breach (August 15, 2019)*, 2019.
- [9] C. Dwork, "Differential privacy: A survey of results," in *Theory and Applications of Models of Computation: 5th International Conference, TAMC*, M. Agrawal, D. Du, and Z. Duan, Eds., 2008, pp. 1–19. [Online]. Available: [https://doi.org/10.1007/978-3-540-79228-4\\_1](https://doi.org/10.1007/978-3-540-79228-4_1)
- [10] Úlfar Erlingsson, V. Pihur, and A. Korolova, "Rappor: Randomized aggregatable privacy-preserving ordinal response," in *Proceedings of the 21st ACM CCS*, 2014. [Online]. Available: <https://arxiv.org/abs/1407.6981>
- [11] A. Greenberg, "Apple's 'differential privacy' is about collecting your data—but not your data," 2016. [Online]. Available: <https://www.wired.com/2016/06/apples-differential-privacy-collecting-data/>
- [12] T. Wang, J. Blocki, N. Li, and S. Jha, "Locally differentially private protocols for frequency estimation," in *26th USENIX Security Symposium (USENIX Security 17)*, USENIX Association, 2017, pp. 729–745. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/wang>
- [13] Z. Qin, Y. Yang, and T. Yu, "Heavy hitter estimation over set-valued data with local differential privacy," in *Proceedings of the 2016 ACM SIGSAC*, ser. CCS '16, 2016, pp. 192–203. [Online]. Available: <http://doi.acm.org/10.1145/2976749.2978409>
- [14] C. Huang, P. Kairouz, X. Chen, L. Sankar, and R. Rajagopal, "Context-aware generative adversarial privacy," *CoRR*, vol. abs/1710.09549, 2017. [Online]. Available: <http://arxiv.org/abs/1710.09549>
- [15] P. Kairouz, S. Oh, and P. Viswanath, "The composition theorem for differential privacy," *IEEE Transactions on Information Theory*, vol. 63, no. 6, pp. 4037–4049, 2017.
- [16] S. L. Warner, "Randomized response: A survey technique for eliminating evasive answer bias," *Journal of the American Statistical Association*, vol. 60, no. 309, pp. 63–69, 1965. [Online]. Available: <http://www.jstor.org/stable/2283137>
- [17] C. Dwork, M. Naor, T. Pitassi, and G. N. Rothblum, "Differential privacy under continual observation," in *Proceedings of the Forty-Second ACM Symposium on Theory of Computing*, ser. STOC '10, New York, NY, USA, 2010, p. 715–724.
- [18] E. Bozkir, O. Günlü, W. Fuhl, R. Schaefer, and E. Kasneci, "Differential privacy for eye tracking with temporal correlations," *PLOS ONE*, vol. 16, p. e0255979, 08 2021.
- [19] R. Bassily, "Linear queries estimation with local differential privacy," *CoRR*, vol. abs/1810.02810, 2018. [Online]. Available: <http://arxiv.org/abs/1810.02810>
- [20] B. Avent, A. Korolova, D. Zeber, T. Hovden, and B. Livshits, "BLENDER: Enabling local search with a hybrid differential privacy model," in *26th USENIX Security Symposium (USENIX Security 17)*. Vancouver, BC: USENIX Association, Aug. 2017, pp. 747–764. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/avent>
- [21] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, "Our data, ourselves: Privacy via distributed noise generation," in *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, ser. Lecture Notes in Computer Science, S. Vaudenay, Ed., vol. 4004. Springer, 2006, pp. 486–503. [Online]. Available: [https://doi.org/10.1007/11761679\\_29](https://doi.org/10.1007/11761679_29)
- [22] M. E. Andrés, N. E. Bordenabe, and K. Chatzikokolakis, "Geo-indistinguishability: Differential privacy for location-based systems," *CoRR*, vol. abs/1212.1984, 2012. [Online]. Available: <https://arxiv.org/pdf/1212.1984.pdf>
- [23] M. S. Alvim, K. Chatzikokolakis, C. Palamidessi, and A. Pazis, "Metric-based local differential privacy for statistical applications," *CoRR*, vol. abs/1805.01456, 2018. [Online]. Available: <http://arxiv.org/abs/1805.01456>
- [24] B. Jiang, M. Li, and R. Tandon, "Context-Aware data aggregation with localized information privacy," in *2018 IEEE Conference on Communications and Network Security (CNS)*, May 2018.
- [25] ——, "Local information privacy with bounded prior," in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, May 2019, pp. 1–7.
- [26] ——, "Local information privacy and its application to privacy-preserving data aggregation," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 3, pp. 1918–1935, 2022.
- [27] ——, "Online context-aware data release with sequence information privacy," 2023.
- [28] B. Jiang, M. Seif, R. Tandon, and M. Li, "Context-aware local information privacy," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3694–3708, 2021.
- [29] M. E. Gursoy, A. Tamersoy, S. Truex, W. Wei, and L. Liu, "Secure and utility-aware data collection with condensed local differential privacy," *CoRR*, vol. abs/1905.06361, 2019. [Online]. Available: <http://arxiv.org/abs/1905.06361>
- [30] Y. NIE, W. Yang, L. Huang, X. Xie, Z. Zhao, and S. Wang, "A utility-optimized framework for personalized private histogram estimation," *IEEE Transactions on Knowledge and Data Engineering*, vol. 31, no. 4, pp. 655–669, 2019.
- [31] T. Murakami and Y. Kawamoto, "Utility-optimized local differential privacy mechanisms for distribution estimation," in *Proceedings of the 28th USENIX Conference on Security Symposium*, ser. SEC'19. USA: USENIX Association, 2019, p. 1877–1894.
- [32] S. Takagi, Y. Cao, and M. Yoshikawa, "Poster: Data collection via local differential privacy with secret parameters," in *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, ser. ASIA CCS '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 910–912. [Online]. Available: <https://doi.org/10.1145/3320269.3405441>