

# Reveal-or-Obscure: A Differentially Private Sampling Algorithm for Discrete Distributions

Naima Tasnim, Atefeh Gilani, Lalitha Sankar and Oliver Kosut  
Arizona State University, Tempe, AZ, USA  
Email: {ntasnim2, agilani2, lsankar, okosut}@asu.edu

**Abstract**—THIS PAPER IS ELIGIBLE FOR THE STUDENT PAPER AWARD. We propose a differentially private algorithm called reveal-or-obscure (ROO) to generate samples from a dataset of  $n$  observations drawn i.i.d. from an unknown discrete distribution  $P$ . Our algorithm outputs a single sample from a distribution that is close to  $P$  in total variation distance. We prove that our proposed method satisfies  $\epsilon$ -differential privacy. The ROO algorithm is distinct from state-of-the-art methods in that it does not explicitly perturb the empirical probability distribution of the given dataset. Relative to such approaches, ROO achieves improved sampling complexity for the same privacy and utility guarantees.

## I. INTRODUCTION

The widespread use of sensitive data across various domains, including healthcare, finance, law enforcement, and social sciences, has heightened the importance of privacy-preserving data analysis. Consequently, there is a growing need for mechanisms that allow data analysis while minimizing individual privacy risks. One promising approach is the use of synthetic data that capture the statistical properties of the original data.

Differential Privacy (DP) [1], [2] has emerged as a sound framework for formalizing privacy guarantees across a range of applications, including data analysis. In essence, DP ensures that the output of an algorithm does not differ by much whether or not an individual's data is included in the input.

The task of synthetic data generation is closely related to the broader problem of learning probability distributions [3]. In the non-private setting, a learning algorithm approximates a distribution from which one can sample new data points that are representative of the original data. When privacy constraints are introduced, learning a distribution becomes significantly more challenging. In many practical cases, it may be sufficient to produce a small number of representative samples instead. The task of privately releasing one sample—known as DP sampling—is easier than full-fledged learning, since it requires less information from the underlying distribution. Motivated by this, we propose a novel DP sampling algorithm for discrete distributions on a finite alphabet. The key idea of our approach is to “obscure” the empirical distribution of the input dataset with a certain probability, or “reveal” it otherwise. Hence, we call our proposed algorithm reveal-or-obscure (ROO).

**Main Contributions.** Our main contributions are:

- We propose ROO—a sampling algorithm that achieves differential privacy without *explicitly* perturbing the empirical distribution of the input dataset. We incorporate

uncertainty in our algorithm by sampling from the uniform distribution with some fixed probability  $q$ .

- We prove that our proposed algorithm reduces the sampling complexity while achieving better privacy-utility trade-off than the state-of-the-art [4].
- We also propose DS-ROO (data-specific ROO) as a technique to generalize ROO by making  $q$ , i.e., the probability of sampling from the uniform distribution, a function of the empirical distribution of the dataset. We prove that it is possible to achieve the same privacy guarantee with a lower  $q$  value relative to the vanilla ROO algorithm for sufficiently large datasets.
- We demonstrate empirically that, for the same privacy guarantee, DS-ROO achieves better utility than vanilla ROO as well as the state-of-the-art in [4].

**Related Work.** The problem of differentially private sampling from unknown distributions is first investigated in [4]. Raskhodnikova *et al.* [4] provide the first known bounds with  $(\epsilon, \delta)$ -DP guarantees on the complexity of sampling from arbitrary distributions over a discrete alphabet. DP algorithms for sampling from higher dimensional distributions such as multivariate Gaussians are presented in [5]. Husain *et al.* [6] considers DP sampling in the local setting, where the central aggregator cannot be trusted and each user must produce a single data record privately. Private sampling has also been studied in the distributed setting [7], [8]. A key focus of these efforts has been to reduce the sample complexity of DP-assured private sampling. Our proposed ROO and DS-ROO improves the best known bounds in [4] under the same settings. More generally, the problem of releasing a dataset in a differentially private manner has also been studied; for example, [9]–[13]. Generating a single sample in a private manner with guarantees is the first step towards releasing a larger synthetic dataset, and to this end, we focus on the former challenge in this paper.

## II. PROBLEM SETUP

We begin by briefly reviewing some relevant definitions. We use uppercase letters, e.g.,  $X$ , to denote random variables (RVs), and lowercase letters, e.g.  $x$ , for their instantiations. We assume that the dataset consists of  $n$  RVs sampled from a finite alphabet of  $k$  letters; without loss of generality, we take this alphabet to be  $[k] = \{1, 2, \dots, k\}$ . Let  $\mathcal{P}$  be the class of probability distributions on  $[k]$ . Given a dataset  $X^n = (X_1, X_2, \dots, X_n)$  of  $n$  i.i.d. observations from some

unknown  $P \in \mathcal{P}$ , a randomized algorithm (privacy mechanism)  $\mathcal{A} : \mathcal{X}^n \mapsto \mathcal{X}$  outputs a single sample from  $\mathcal{X}$ . Let  $Y = \mathcal{A}(X^n)$  be the random variable corresponding to the output of algorithm  $\mathcal{A}$  given input  $X^n$ . The output  $\mathcal{A}(X^n)$  is drawn from a distribution  $Q$  such that

$$Q(y) = \sum_{x^n \in \mathcal{X}^n} \Pr\{\mathcal{A}(x^n) = y | x^n\} \Pr\{X^n = x^n\}. \quad (1)$$

The accuracy of  $\mathcal{A}$  is measured by the *closeness* between  $Q$  and  $P$ . We use the *total variation distance*, defined as

$$d_{TV}(Q, P) = \frac{1}{2} \|Q - P\|_1 = \frac{1}{2} \sum_x |Q(x) - P(x)|. \quad (2)$$

We use the following definition of sampling accuracy, introduced in [14].

**Definition 1 (Accuracy of Sampling [14]):** An algorithm  $\mathcal{A}$  is  $\alpha$ -accurate on a distribution  $P$  if the total variation distance,  $d_{TV}$  between  $Q$  and  $P$  is bounded by some constant  $\alpha$ , i.e.,

$$d_{TV}(Q, P) \leq \alpha. \quad (3)$$

An algorithm is  $\alpha$ -accurate on a class  $\mathcal{P}$  of distributions if it is  $\alpha$ -accurate on every  $P \in \mathcal{P}$ .

Two datasets  $x^n$  and  $\tilde{x}^n$  are considered *neighbors*, denoted  $x^n \sim \tilde{x}^n$ , if they differ by at most one entry. DP is defined with respect to all such neighboring datasets as follows.

**Definition 2 (Differential Privacy [1]):** A randomized algorithm, or mechanism  $\mathcal{A} : \mathcal{X}^n \rightarrow \mathcal{Y}$  is considered  $\epsilon$ -differentially private ( $\epsilon$ -DP) if, for every pair of neighboring datasets  $x^n \sim \tilde{x}^n \in \mathcal{X}^n$ , and for all  $Y \subseteq \mathcal{Y}$ ,

$$\Pr\{\mathcal{A}(x^n) \in Y\} \leq e^\epsilon \Pr\{\mathcal{A}(\tilde{x}^n) \in Y\}. \quad (4)$$

In [4], the authors present an achievable  $\epsilon$ -DP sampler which does the following:

- (i) computes, for each  $j \in [k]$ , the empirical probability distribution  $\hat{p}_j$ ,
- (ii) adds Laplace noise to each count,
- (iii) uses an  $L_1$  projection to restrict the Laplace-noised distribution to be a probability vector  $\tilde{P} = (\tilde{p}_1, \dots, \tilde{p}_k)$ , and
- (iv) outputs an element of  $[k]$  sampled from the distribution  $\tilde{P}$ .

For this algorithm, they show that for a sampling complexity

$$n' = \frac{2k}{\alpha\epsilon}, \quad (5)$$

their algorithm is  $\alpha$ -accurate. In the following section, we prove that it is possible to achieve an  $\epsilon$ -DP and  $\alpha$ -accurate sampler with fewer samples than  $n'$ . Notably, for higher values of  $\epsilon$ , i.e., lower privacy, we gain an exponential reduction in the required number of samples. Moreover, [4] also presented a lower bound on the sampling complexity as  $\Omega(\frac{k}{\alpha\epsilon})$  for a restricted range of  $\epsilon \in (0, 1]$ .

### III. REVEAL-OR-OBSCURE (ROO)

Fig 1 presents our proposed private sampling algorithm ROO. We implement the idea of obscuring the empirical distribution  $\hat{P}_{x^n}$  by sampling from the uniform distribution

on  $[k]$ . However, we wish to do so with a small probability  $q$ , so that we do not deviate too much from the true distribution  $P$ . With probability  $1 - q$ , we simply choose a sample from the given dataset, i.e., we reveal  $\hat{P}_{x^n}$ .

**Input:** Dataset  $x^n = (x_1, \dots, x_n)$ , alphabet size  $k$ , privacy budget  $\epsilon$ , parameter  $q$

**Output:** Sample  $y$

- 1: With probability  $q$ , choose  $y \sim \text{Unif}[1 : k]$ ;
- 2: Otherwise, pick  $i \sim \text{Unif}[1 : n]$  and choose  $y = x_i$ ;
- 3: **return**  $y$ ;

Fig. 1. The reveal-or-obscure (ROO) algorithm

The privacy and utility guarantees provided by ROO is given by the following theorem.

**Theorem 1:** Given  $q$ , ROO is  $\epsilon$ -DP and  $\alpha$ -accurate for

$$\epsilon = \log \left( 1 + \frac{k(1-q)}{nq} \right), \text{ and} \quad (6)$$

$$\alpha = q \left( 1 - \frac{1}{k} \right), \quad (7)$$

from which we can solve for  $q$  to obtain the sampling complexity as

$$n = \frac{k(1-\alpha) - 1}{\alpha(e^\epsilon - 1)}. \quad (8)$$

**Lemma 1:** For any  $k \geq 2, \epsilon > 0$ , and  $\alpha \in (0, 1 - \frac{1}{k})$ , the sampling complexity of ROO is lower than that of [4], stated in (5).

The proofs of Theorem 1 and Lemma 1 are in Appendix A and B.

In fact, the sampling complexity of ROO is exponentially better in terms of  $\epsilon$  compared to that of [4] in (5). This would appear to violate their lower bound on the sampling complexity; the reason it does not is that their lower bound only applies for  $\epsilon < 1$ .

### IV. DATA-SPECIFIC REVEAL-OR-OBSCURE (DS-ROO)

For the ROO algorithm in Section III, we fix  $q$  in order to achieve  $\epsilon$ -DP for any possible dataset. Recall from (27) in the privacy analysis of Appendix A that the supremum of ratio of probabilities is achieved by setting  $p = 0$ . This corresponds to the case where one of two neighboring datasets under consideration is entirely missing an element of the alphabet, but this element is present in the other dataset. Thus, ROO is inefficient on datasets where each element of the alphabet appears reasonably often. In this section, we show that by making  $q$  a function of the dataset—specifically, a function of the smallest empirical probability, the accuracy can be improved for the same privacy. Let  $m \in \{0, 1, \dots, \lfloor \frac{n}{k} \rfloor\}$  denote the smallest number of times an element of  $[k]$  appears in dataset  $x^n$ . Mathematically,  $m$  can be expressed as  $m = n \cdot \min_x \hat{P}_{x^n}(x)$ . The modified private sampling algorithm—which we call the data-specific reveal-or-obscure (DS-ROO)—is presented in Fig 2. In DS-ROO, the probability  $q_m$  is determined from the value of  $m$  associated with the

given dataset. Notably, when  $m = 0$ , the corresponding  $q_0$  is equivalent to that of ROO in Fig 1. That is, the case of a dataset that is missing an element of the alphabet (so  $m = 0$ ) is the worst-case scenario, and so in this case DS-ROO behaves identically to ROO. However, we will show empirically that in other cases, DS-ROO can do much better than vanilla ROO.

**Input:** Dataset  $x^n = (x_1, \dots, x_n)$ , alphabet size  $k$ , privacy budget  $\epsilon$

**Output:** Sample  $y$

- 1: Compute  $m = n \cdot \min_x \hat{P}_{x^n}(x)$ ;
- 2: Compute

$$q_0 = \frac{1}{1 + \frac{n}{k}(e^\epsilon - 1)}; \quad (9)$$

- 3: **for**  $m = 1, 2, \dots, \lfloor \frac{n}{k} \rfloor$  **do**
- 4:   Compute

$$u_m = -\frac{m}{n} + \frac{1}{k} - \frac{1}{n}, \quad (10)$$

$$v_m = e^\epsilon \left( \frac{1}{k} - \frac{m}{n} \right), \quad (11)$$

$$w_m = -\frac{1}{n} - \frac{m}{n} + \frac{m}{n} e^\epsilon, \quad (12)$$

$$q_m = \max \left\{ 0, \frac{u_m}{v_m} q_{m-1} - \frac{w_m}{v_m} \right\}; \quad (13)$$

- 5: **end for**
- 6: With probability  $q_m$ , choose  $y \sim \text{Unif}[1 : k]$ ;
- 7: Otherwise, pick  $i \sim \text{Unif}[1 : n]$  and choose  $y = x_i$ ;
- 8: **return**  $y$ ;

Fig. 2. The data-specific ROO (DS-ROO) algorithm

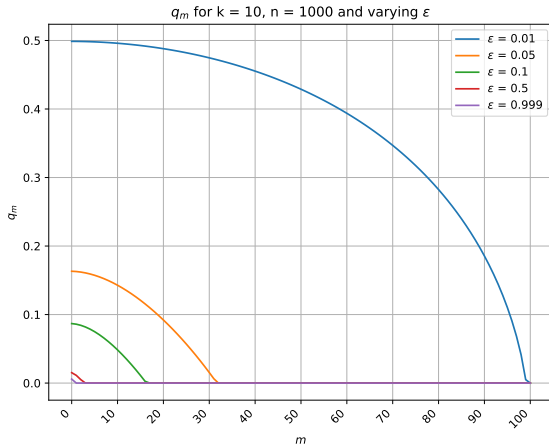


Fig. 3. Plot of  $q_m$  as a function of  $m$  for fixed  $k$  and  $n$ , showing changes under different privacy budgets  $\epsilon$ .

Fig. 3 shows the function  $q_m$  for  $k = 9, n = 1000$ , and several different values of the privacy parameter  $\epsilon$ . We observe that  $q_m$  is non-increasing in  $m$ . As  $m$  increases, the empirical distribution of the dataset gets closer to the uniform distribution, and  $q_m$  approaches zero. Thus, DS-ROO is less

likely to obscure the empirical distribution for larger  $m$ . In high privacy regimes,  $q_m$  tends to decrease much slower. On the other hand, for larger  $\epsilon$ , i.e., low privacy,  $q_m$  goes to zero much faster. The privacy guarantee provided by DS-ROO is given by the following theorem.

**Theorem 2:** The DS-ROO sampling algorithm is  $\epsilon$ -differentially private.

Due to space limitations, the full proof of Theorem 2 is omitted, but it can be found in Appendix C. We provide a proof sketch below.

*Proof Sketch:* Recall that  $m$  denotes the smallest number of times an element of the alphabet  $[k]$  appears in  $x^n$ . For neighboring datasets  $x^n \sim \tilde{x}^n$ , there are three possible values of  $\tilde{m}$ : (1)  $\tilde{m} = m$ , (2)  $\tilde{m} = m + 1$ , and (3)  $\tilde{m} = m - 1$ . Considering each of these cases separately and applying Definition 2, we derive the conditions under which DS-ROO satisfies  $\epsilon$ -DP,

$$q_m \geq \frac{w_m}{u_m - v_m}, \text{ for } m = 0, 1, \dots, \left\lfloor \frac{1}{e^\epsilon - 1} \right\rfloor, \quad (14)$$

$$u_m q_{m+1} \leq v_m q_m + w_m, \text{ for } m = 0, 1, \dots, \left\lfloor \frac{n}{k} \right\rfloor - 1, \quad (15)$$

$$u_m q_{m-1} \leq v_m q_m + w_m, \text{ for } m = 1, 2, \dots, \left\lfloor \frac{n}{k} \right\rfloor, \quad (16)$$

where  $u_m, v_m$ , and  $w_m$  are as defined in (10)–(12). Additionally, for  $q_m$  to be a valid probability, we must also have  $0 \leq q_m \leq 1$  for all  $m$ . Setting the initial value  $q_0$  as in (9), assuming (16) to be an equality, we arrive at the expression

$$q_m = \max \left\{ 0, \frac{u_m}{v_m} q_{m-1} - \frac{w_m}{v_m} \right\}. \quad (17)$$

We can show that the above form of  $q_m$  satisfies the inequality conditions in (14) and (15). Therefore, DS-ROO is  $\epsilon$ -differentially private. ■

#### A. Utility of DS-ROO

We do not have theoretical bounds on the utility of DS-ROO at this time. However, we provide empirical evidence that DS-ROO achieves better utility than vanilla ROO and the state-of-the-art sampler in [4] for the same privacy guarantee. In order to measure the utility of DS-ROO, we consider an input distribution, estimate the corresponding output distribution according to Fig 2, and compute the total variation distance. Fig. 4 shows an example case for a distribution on an alphabet of size  $k = 9$ , with dataset size  $n = 1000$ , and privacy parameter  $\epsilon = 0.1$ . We observe that mixing with the uniform distribution shifts some of the weight from the most probable central element to those with lower probabilities, resulting in reduced skewness in the output distribution.

Recall from Definition 1 that the total variation distance is upper bounded by  $\alpha$ . The smaller the value of  $\alpha$ , the more accurate the sampler is. From (5), the accuracy of the state-of-the-art sampler in [4] is

$$\alpha = \frac{2k}{n'\epsilon}. \quad (18)$$

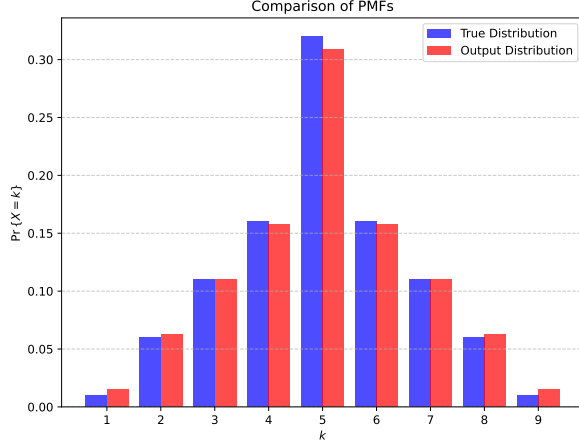


Fig. 4. Comparison of true distribution and the estimated output distribution for DS-ROO.

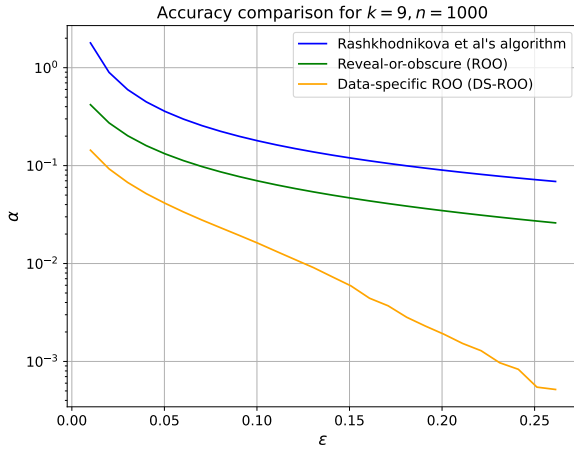


Fig. 5. Comparison of accuracy ( $\alpha$ ) versus privacy ( $\epsilon$ ) curves of differentially private sampling algorithms.

From Theorem 1, we have the accuracy of ROO

$$\alpha = \frac{1}{1 + \frac{n}{k}(e^\epsilon - 1)}. \quad (19)$$

For fixed values of  $k$  and  $n$ , we obtain the accuracy of DS-ROO empirically, and compare it with that of [4] and ROO. Fig. 5 shows the  $\alpha$  vs.  $\epsilon$  curves for all three algorithms. We observe that DS-ROO achieves dramatically better accuracy than [4] and vanilla ROO while providing the same privacy guarantee. Of course, the numerical results in Fig. 5 are for the particular distribution shown in Fig. 4. We anticipate that we will see similar improvements for distributions that are not too skewed—if the distribution is more skewed (such as if the probability of a letter is 0), then there will be no improvement over vanilla ROO.

## V. CONCLUSION

In this work, we propose a novel differentially private sampling algorithm for discrete distributions on a finite alphabet. Our algorithm achieves differential privacy by obscuring

the empirical distribution of a dataset without perturbing it directly. In addition, we propose a method to generalize our approach to achieve better utility for the same privacy guarantee. For future work, we aim to explore the practicality of our proposed algorithms for more complex distribution classes.

## APPENDIX

### A. Proof of Theorem 1

**Privacy Analysis.** Given  $x^n$ , the ROO algorithm in Fig 1 chooses output  $Y = y$  with probability

$$P(Y = y|x^n) = \frac{q}{k} + (1 - q)\hat{P}_{x^n}(y), \quad (20)$$

where  $\hat{P}_{x^n}(x)$  denotes the empirical probability of each  $x \in [k]$ ,

$$\hat{P}_{x^n}(x) = \frac{1}{n} \sum_{i=1}^n \mathbf{1}(x_i = x). \quad (21)$$

For neighboring datasets  $x^n \sim \tilde{x}^n$ , their corresponding empirical probabilities of one observation differ by at most  $\frac{1}{n}$ , i.e., for all  $x \in \mathcal{X}$ ,

$$|\hat{P}_{x^n}(x) - \hat{P}_{\tilde{x}^n}(x)| \leq \frac{1}{n}. \quad (22)$$

By Definition 2, in order for ROO to satisfy  $\epsilon$ -DP, the following condition must hold for all possible  $x^n \sim \tilde{x}^n$ ,

$$\frac{P(Y = y|x^n)}{P(Y = y|\tilde{x}^n)} \leq e^\epsilon. \quad (23)$$

We can write the left side of (23) as

$$\frac{P(Y = y|x^n)}{P(Y = y|\tilde{x}^n)} = \frac{\frac{q}{k} + (1 - q)\hat{P}_{x^n}(y)}{\frac{q}{k} + (1 - q)\hat{P}_{\tilde{x}^n}(y)} \quad (24)$$

$$\leq \sup_p \frac{\frac{q}{k} + (1 - q)(p + \frac{1}{n})}{\frac{q}{k} + (1 - q)p} \quad (25)$$

$$= \sup_p 1 + \frac{(1 - q)\frac{1}{n}}{\frac{q}{k} + (1 - q)p} \quad (26)$$

$$\leq 1 + \frac{(1 - q)\frac{1}{n}}{\frac{q}{k}}. \quad (27)$$

Here, in (24), we substitute (20). In (25), we use the property of the empirical probabilities stated in (22), denoting  $\hat{P}_{\tilde{x}^n}(y)$  with  $p$  for notational simplicity. In (27), the supremum is obtained when  $p = 0$ . Therefore, ROO satisfies  $\epsilon$ -DP guarantee if the right side of (27) is bounded by  $e^\epsilon$ , i.e.,

$$1 + \frac{(1 - q)\frac{1}{n}}{\frac{q}{k}} \leq e^\epsilon. \quad (28)$$

Rearranging (28), we obtain the privacy guarantee of Theorem 1 stated in (6).

**Utility Analysis.** For our proposed sampler ROO in Fig 1, the output distribution is

$$Q(y) = \sum_{x^n \in \mathcal{X}^n} \left( \frac{q}{k} + (1-q)\hat{P}_{x^n}(y) \right) \Pr\{X^n = x^n\} \quad (29)$$

$$= \frac{q}{k} \sum_{x^n \in \mathcal{X}^n} \Pr\{X^n = x^n\} + (1-q) \sum_{x^n \in \mathcal{X}^n} \hat{P}_{x^n}(y) \Pr\{X^n = x^n\} \quad (30)$$

$$= \frac{q}{k} + (1-q)\mathbb{E}_{X^n}[\hat{P}_{x^n}(y)] \quad (31)$$

$$= \frac{q}{k} + (1-q)P(y), \quad (32)$$

where (32) follows from the fact that  $\hat{P}_{x^n}$  is the empirical distribution of a dataset sampled from  $P$ . The total variation distance between the discrete distributions  $Q$  and  $P$  is thus

$$d_{TV}(Q, P) = \frac{1}{2} \sum_{y \in \mathcal{X}} |Q(y) - P(y)| \quad (33)$$

$$= \frac{q}{2} \sum_{y \in \mathcal{X}} \left| \frac{1}{k} - P(y) \right| \quad (34)$$

$$= q \times d_{TV}\left(\frac{1}{k}, P(y)\right) \quad (35)$$

$$\leq q \times \max_{P(y)} d_{TV}\left(\frac{1}{k}, P(y)\right), \quad (36)$$

where we obtain (34) by rearranging and substituting (32). Note that, for a convex objective function, the maximum is achieved at its corner points. Hence, the distribution  $P$  that maximizes the  $d_{TV}$  between the uniform distribution on  $[k]$  and the input distribution  $P$  must be one of the corner points of the  $k$ -dimensional probability simplex  $\mathcal{P}$ , e.g.  $P = \{1, 0, \dots, 0\}$ . The maximum  $d_{TV}$  is then computed as

$$\max_{P(y)} d_{TV}\left(\frac{1}{k}, P(y)\right) = \max_{P(y)} \frac{1}{2} \sum_{y \in \mathcal{X}} \left| \frac{1}{k} - P(y) \right| \quad (37)$$

$$= 1 - \frac{1}{k}. \quad (38)$$

Substituting this maximum objective value into (36), we have

$$d_{TV}(Q, P) \leq q \left(1 - \frac{1}{k}\right). \quad (39)$$

Comparing this result with Definition 1, we obtain the utility of Theorem 1 stated in (7). We can then express  $q$ , i.e., the probability of sampling from the uniform distribution, in terms of  $\alpha$  and  $k$ ,

$$q = \frac{\alpha}{1 - \frac{1}{k}} = \frac{k\alpha}{k-1}. \quad (40)$$

Substituting the above into (28) and rearranging, we obtain sample complexity

$$n = \frac{k(1-\alpha) - 1}{\alpha(e^\epsilon - 1)}. \quad (41)$$

## B. Proof of Lemma 1

From Theorem 1, we have the sampling complexity of ROO,

$$n = \frac{k(1-\alpha) - 1}{\alpha(e^\epsilon - 1)} = \frac{k(1-\alpha - \frac{1}{k})}{\alpha(e^\epsilon - 1)} \quad (42)$$

$$= \frac{2k}{\alpha\epsilon} \frac{\epsilon}{2(e^\epsilon - 1)} \left(1 - \frac{1}{k} - \alpha\right) \quad (43)$$

$$< \frac{2k}{\alpha\epsilon} = n'. \quad (44)$$

As  $\epsilon$  increases, the term  $e^\epsilon - 1$  in the denominator of (8) grows exponentially, resulting in significantly lower  $n$  compared to  $n'$ .

## C. Proof of Theorem 2

Since  $m$  denotes the smallest number of times an element in the alphabet  $[k]$  appears in a dataset  $x^n$ , it is at most  $\lfloor \frac{n}{k} \rfloor$  when the empirical distribution is uniform. For neighboring datasets  $x^n \sim \tilde{x}^n$ , there are three possible values of  $\tilde{m}$ : (1)  $\tilde{m} = m$ , when the different entry in  $\tilde{x}^n$  is a different element in  $[k]$ , hence it does not affect the minimum count, (2)  $\tilde{m} = m + 1$ , and (3)  $\tilde{m} = m - 1$ . In order to understand how the behavior of  $q_m$  changes with  $m$ , we first analyze the likelihood ratio of the output distributions. Recall from Definition 2 that, for Fig 2 to achieve  $\epsilon$ -DP, the following condition must hold for all possible  $x^n \sim \tilde{x}^n$  pairs,

$$\max_x \frac{\frac{q_{\tilde{m}}}{k} + (1 - q_{\tilde{m}})\hat{P}_{\tilde{x}^n}(x)}{\frac{q_m}{k} + (1 - q_m)\hat{P}_{x^n}(x)} \leq e^\epsilon. \quad (45)$$

Adding and subtracting  $\hat{P}_{x^n}(x)$  from  $\hat{P}_{\tilde{x}^n}(x)$  in the numerator, the condition becomes

$$\max_x \frac{\frac{q_{\tilde{m}}}{k} + (1 - q_{\tilde{m}})(\hat{P}_{\tilde{x}^n}(x) - \hat{P}_{x^n}(x) + \hat{P}_{x^n}(x))}{\frac{q_m}{k} + (1 - q_m)\hat{P}_{x^n}(x)} \leq e^\epsilon. \quad (46)$$

The ratio is maximized when the numerator is maximized. Using (22), we can rewrite the condition as

$$\frac{\frac{q_{\tilde{m}}}{k} + (1 - q_{\tilde{m}})(\frac{1}{n} + \hat{P}_{x^n}(x))}{\frac{q_m}{k} + (1 - q_m)\hat{P}_{x^n}(x)} \leq e^\epsilon \quad (47)$$

$$\Rightarrow \hat{P}_{x^n}(x) (1 - q_{\tilde{m}} - e^\epsilon(1 - q_m)) \leq e^\epsilon \frac{q_m}{k} - \frac{q_{\tilde{m}}}{k} - (1 - q_{\tilde{m}}) \frac{1}{n}. \quad (48)$$

Assuming  $q_m$  and  $q_{\tilde{m}}$  do not change significantly for  $x^n \sim \tilde{x}^n$ , we require

$$1 - q_{\tilde{m}} < e^\epsilon(1 - q_m) \Rightarrow 1 - q_{\tilde{m}} - e^\epsilon(1 - q_m) < 0. \quad (49)$$

Then, the inequality in (48) becomes

$$\hat{P}_{x^n}(x) \geq \frac{e^\epsilon \frac{q_m}{k} - \frac{q_{\tilde{m}}}{k} - (1 - q_{\tilde{m}}) \frac{1}{n}}{1 - q_{\tilde{m}} - e^\epsilon(1 - q_m)}. \quad (50)$$

If (50) holds for all  $x \in \mathcal{X}$ , it must also hold for the minimum value of  $\hat{P}_{x^n}(x)$ , i.e.,

$$\frac{m}{n} \geq \frac{e^\epsilon \frac{q_m}{k} - \frac{q_{\tilde{m}}}{k} - (1 - q_{\tilde{m}}) \frac{1}{n}}{1 - q_{\tilde{m}} - e^\epsilon(1 - q_m)}. \quad (51)$$



Simplifying (51), we arrive at the condition

$$\left(-\frac{m}{n} + \frac{1}{k} - \frac{1}{n}\right) q_{\tilde{m}} \leq e^\epsilon \left(\frac{1}{k} - \frac{m}{n}\right) q_m - \frac{1}{n} - \frac{m}{n} + \frac{m}{n} e^\epsilon, \quad (52)$$

$$\Rightarrow u_m q_{\tilde{m}} \leq v_m q_m + w_m, \quad (53)$$

where  $u_m, v_m$  and  $w_m$  are as defined in (10)–(12). Now, for  $\tilde{m} = m$ , we can replace  $q_{\tilde{m}}$  with  $q_m$  to obtain

$$q_m \geq \frac{w_m}{u_m - v_m}. \quad (54)$$

Since the denominator is always negative, the right side of (54) will be positive only when the numerator is also negative, i.e.,

$$w_m = -\frac{1}{n} - \frac{m}{n} + \frac{m}{n} e^\epsilon < 0 \Rightarrow m < \frac{1}{e^\epsilon - 1}. \quad (55)$$

For  $\tilde{m} = m + 1$  and  $\tilde{m} = m - 1$ , we obtain two more inequalities,

$$u_m q_{m+1} \leq v_m q_m + w_m, \quad (56)$$

$$u_m q_{m-1} \leq v_m q_m + w_m. \quad (57)$$

Therefore, for Fig 2 to achieve  $\epsilon$ -DP, the function  $q_m$  must satisfy the inequalities in (54), (56), and (57). Defining the initial value  $q_0$  as in (9), and assuming (57) to be an equality for  $m \geq 1$ , we arrive at the expression

$$q_m = \frac{u_m}{v_m} q_{m-1} - \frac{w_m}{v_m}. \quad (58)$$

Note that, since  $q_m$  is a probability, we must have  $0 \leq q_m \leq 1$  for all  $m$ . Therefore, (58) is valid only when the right side is positive. The final form of  $q_m$  is thus

$$q_m = \max \left\{ 0, \frac{u_m}{v_m} q_{m-1} - \frac{w_m}{v_m} \right\}. \quad (59)$$

The proofs of (58) satisfying the conditions in (54) and (56) are provided in Lemma 4 and 3. The proof that the function  $q_m$  is non-increasing is provided in Lemma 2. When  $m = 0$ ,  $q_m$  is equal to that of the fixed  $q$  of Fig 1. As  $m$  increases, the input distribution gets closer to  $\text{Unif}[1 : k]$ , and Fig 2 obscures the output distribution with smaller probability.

#### D. More Proofs

**Lemma 2:** For any  $k \geq 2, \epsilon > 0$ , and datasets of size  $n$  where  $n \gg k$ , the function  $q_m$  is non-increasing.

*Proof:* Since the function  $q_m : \{0, 1, \dots, \lfloor \frac{n}{k} \rfloor\} \mapsto [0, 1]$  is discrete, we need to show that

$$q_m \leq q_{m-1}, \quad (60)$$

for all  $m \in \{0, 1, \dots, \lfloor \frac{n}{k} \rfloor\}$ . From Section IV, we have, for  $m \geq 1$  and positive  $q_m$ ,

$$v_m q_m = u_m q_{m-1} - w_m \quad (61)$$

$$\Rightarrow v_m q_m - v_m q_{m-1} = u_m q_{m-1} - w_m - v_m q_{m-1} \quad (62)$$

$$\Rightarrow q_m - q_{m-1} = \frac{u_m - v_m}{v_m} q_{m-1} - \frac{w_m}{v_m} \quad (63)$$

$$\Rightarrow q_m - q_{m-1} = \left( \frac{u_m}{v_m} - 1 \right) q_{m-1} - \frac{w_m}{v_m}. \quad (64)$$

It suffices to show that the right side of (64) is negative. Substituting (10) and (11) into the first coefficient, we have

$$\frac{u_m}{v_m} - 1 = \frac{-\frac{m}{n} + \frac{1}{k} - \frac{1}{n}}{e^\epsilon \left( \frac{1}{k} - \frac{m}{n} \right)} - 1 \quad (65)$$

$$= \frac{\left( \frac{1}{k} - \frac{m}{n} \right) \frac{1}{n} - e^\epsilon \left( \frac{1}{k} - \frac{m}{n} \right)}{e^\epsilon \left( \frac{1}{k} - \frac{m}{n} \right)} \quad (66)$$

$$= \frac{-\frac{1}{n} - \left( \frac{1}{k} - \frac{m}{n} \right) (e^\epsilon - 1)}{e^\epsilon \left( \frac{1}{k} - \frac{m}{n} \right)} \quad (67)$$

$$< 0. \quad (68)$$

Similarly, substituting (12) into the second coefficient, we have

$$\frac{w_m}{v_m} = \frac{-\frac{1}{n} - \frac{m}{n} + \frac{m}{n} e^\epsilon}{e^\epsilon \left( \frac{1}{k} - \frac{m}{n} \right)} \quad (69)$$

$$= \frac{-\frac{1}{n} + \frac{m}{n} (e^\epsilon - 1)}{e^\epsilon \left( \frac{1}{k} - \frac{m}{n} \right)} \quad (70)$$

$$> 0, \quad (71)$$

for  $m > \lfloor \frac{1}{e^\epsilon - 1} \rfloor$ . Since  $q_m$  has a lower bound 0 in this range, the right side of (64) is

$$\left( \frac{u_m}{v_m} - 1 \right) q_{m-1} - \frac{w_m}{v_m} < 0. \quad (72)$$

It still remains to show that  $q_m - q_{m-1} < 0$  for  $m = 1, 2, \dots, \lfloor \frac{1}{e^\epsilon - 1} \rfloor$ . Recall from (54) in Appendix C that, in this range of  $m$ ,  $q_m$  has a non-zero, positive lower bound. Substituting this bound to the right side of (64), we have

$$\begin{aligned} & \left( \frac{u_m}{v_m} - 1 \right) \frac{w_{m-1}}{u_{m-1} - v_{m-1}} - \frac{w_m}{v_m} \\ &= \frac{-\frac{1}{n} - \left( \frac{1}{k} - \frac{m}{n} \right) (e^\epsilon - 1)}{e^\epsilon \left( \frac{1}{k} - \frac{m}{n} \right)} \frac{\frac{m-1}{n} (e^\epsilon - 1) - \frac{1}{n}}{\left( \frac{m-1}{n} - \frac{1}{k} \right) (e^\epsilon - 1) - \frac{1}{n}} - \frac{w_m}{v_m} \end{aligned} \quad (73)$$

$$= \frac{-\frac{1}{n} - \left( \frac{1}{k} - \frac{m}{n} \right) (e^\epsilon - 1)}{\left( \frac{m-1}{n} - \frac{1}{k} \right) (e^\epsilon - 1) - \frac{1}{n}} \frac{\frac{m-1}{n} (e^\epsilon - 1) - \frac{1}{n}}{e^\epsilon \left( \frac{1}{k} - \frac{m}{n} \right)} - \frac{w_m}{v_m} \quad (74)$$

$$= C \frac{-\frac{1}{n} + \frac{m}{n} (e^\epsilon - 1) - \frac{1}{n} (e^\epsilon - 1)}{e^\epsilon \left( \frac{1}{k} - \frac{m}{n} \right)} - \frac{w_m}{v_m} \quad (75)$$

$$= C \left[ \frac{-\frac{1}{n} + \frac{m}{n} (e^\epsilon - 1)}{e^\epsilon \left( \frac{1}{k} - \frac{m}{n} \right)} - \frac{\frac{1}{n} (e^\epsilon - 1)}{e^\epsilon \left( \frac{1}{k} - \frac{m}{n} \right)} \right] - \frac{w_m}{v_m} \quad (76)$$

$$= C \left[ \frac{w_m}{v_m} - \frac{e^\epsilon - 1}{e^\epsilon \left( \frac{n}{k} - m \right)} \right] - \frac{w_m}{v_m}. \quad (77)$$

Here,  $\frac{w_m}{v_m} < 0$  for the relevant range of  $m$ . Moreover, since  $\frac{n}{k} > m$ ,  $\frac{e^\epsilon - 1}{e^\epsilon \left( \frac{n}{k} - m \right)}$  is positive and less than 1. Finally, the coefficient,

$$C = \frac{-\frac{1}{n} - \left( \frac{1}{k} - \frac{m}{n} \right) (e^\epsilon - 1)}{\left( \frac{m-1}{n} - \frac{1}{k} \right) (e^\epsilon - 1) - \frac{1}{n}} \quad (78)$$

$$= \frac{-\frac{1}{n} - \left( \frac{1}{k} - \frac{m-1+1}{n} \right) (e^\epsilon - 1)}{\left( \frac{m-1}{n} - \frac{1}{k} \right) (e^\epsilon - 1) - \frac{1}{n}} \quad (79)$$

$$= \frac{\left( \frac{m-1}{n} - \frac{1}{k} \right) (e^\epsilon - 1) - \frac{1}{n} + \frac{1}{n} (e^\epsilon - 1)}{\left( \frac{m-1}{n} - \frac{1}{k} \right) (e^\epsilon - 1) - \frac{1}{n}} \quad (80)$$

$$\begin{aligned}
&= 1 + \frac{\frac{1}{n}(e^\epsilon - 1)}{\left(\frac{m-1}{n} - \frac{1}{k}\right)(e^\epsilon - 1) - \frac{1}{n}} \\
&= 1 - \frac{e^\epsilon - 1}{1 + n(e^\epsilon - 1)\left(\frac{1}{k} - \frac{m-1}{n}\right)} \\
&< 1.
\end{aligned} \tag{81}$$

Therefore, we have

$$\begin{aligned}
&C \left[ \frac{w_m}{v_m} - \frac{e^\epsilon - 1}{e^\epsilon \left(\frac{n}{k} - m\right)} \right] < \frac{w_m}{v_m} \\
\Rightarrow C \left[ \frac{w_m}{v_m} - \frac{e^\epsilon - 1}{e^\epsilon \left(\frac{n}{k} - m\right)} \right] - \frac{w_m}{v_m} < 0
\end{aligned} \tag{84}$$

Thus, for all  $m$ ,

$$q_m \leq q_{m-1}, \tag{86}$$

i.e.,  $q_m$  is non-increasing.  $\blacksquare$

*Lemma 3:* For  $m \in \{0, 1, \dots, \lfloor \frac{n}{k} \rfloor - 1\}$ , the function  $q_m$  satisfies the inequality condition

$$u_m q_{m+1} < v_m q_m + w_m. \tag{87}$$

*Proof:* Using (10)–(12), we have, for  $m = 0$ ,

$$u_0 = \frac{1}{k} - \frac{1}{n}, v_0 = \frac{e^\epsilon}{k}, w_0 = -\frac{1}{n}. \tag{88}$$

Then, we can write

$$\begin{aligned}
u_0 q_1 - v_0 q_0 &= u_0 q_1 - u_0 q_0 + u_0 q_0 - v_0 q_0 \\
&= u_0 (q_1 - q_0) + \left(\frac{1}{k} - \frac{1}{n}\right) q_0 - \frac{e^\epsilon}{k} q_0
\end{aligned} \tag{89}$$

$$= u_0 (q_1 - q_0) + \left(\frac{1}{k} + w_0\right) q_0 - \frac{e^\epsilon}{k} q_0 \tag{90}$$

$$= u_0 (q_1 - q_0) + \frac{1}{k} q_0 + w_0 q_0 - \frac{e^\epsilon}{k} q_0 \tag{91}$$

$$= w_0 q_0 - \frac{e^\epsilon - 1}{k} q_0 - u_0 (q_0 - q_1) \tag{92}$$

$$< w_0. \tag{93}$$

Here, (93) follows from the fact that  $0 \leq q_0 \leq 1$  and  $q_m$  is non-increasing.

For  $m = 1, 2, \dots, \lfloor \frac{n}{k} \rfloor - 1$ , we can write

$$u_m q_{m+1} - v_m q_m = u_m q_{m+1} - u_m q_{m-1} + w_m \tag{94}$$

$$= w_m + u_m (q_{m+1} - q_{m-1}) \tag{95}$$

$$= w_m + \left(-\frac{m}{n} + \frac{1}{k} - \frac{1}{n}\right) (q_{m+1} - q_{m-1}) \tag{96}$$

$$= w_m - \left(\frac{1}{k} - \frac{m+1}{n}\right) (q_{m-1} - q_{m+1}) \tag{97}$$

$$< w_m. \tag{98}$$

Here, in (94), we substitute (58). (98) follows from the fact that  $q_m$  is non-increasing and  $\frac{1}{k} - \frac{m+1}{n}$  is non-negative for  $m = 1, 2, \dots, \lfloor \frac{n}{k} \rfloor - 1$ . Finally, for  $q_{m+1} = 0$ , we have

$$-v_m q_m = w_m - \left(\frac{1}{k} - \frac{m+1}{n}\right) q_{m-1} \tag{99}$$

$$< w_m \tag{100}$$

$$\Rightarrow q_m > -\frac{w_m}{v_m}. \tag{101}$$

It follows from (71) that the right side of (101) is negative. Thus, (101) is a valid inequality, and we can conclude that  $q_m$  satisfies (87) for the relevant range of  $m$ .  $\blacksquare$

*Lemma 4:* For  $m = 1, 2, \dots, \lfloor \frac{1}{e^\epsilon - 1} \rfloor$ , and  $u_m, v_m$ , the function  $q_m$  satisfies the inequality condition

$$q_m > \frac{w_m}{u_m - v_m}. \tag{102}$$

*Proof:* Let,

$$t_m = \frac{w_m}{u_m - v_m} = \frac{\frac{w_m}{v_m}}{\frac{u_m}{v_m} - 1} \tag{103}$$

$$\Rightarrow \left(\frac{u_m}{v_m} - 1\right) t_m = \frac{w_m}{v_m}. \tag{104}$$

We observe that

$$t_0 = \frac{w_0}{u_0 - v_0} = \frac{-\frac{1}{n}}{\frac{1}{k} - \frac{1}{n} - \frac{e^\epsilon}{k}} = \frac{1}{1 + \frac{n}{k}(e^\epsilon - 1)} = q_0. \tag{105}$$

Moreover,

$$t_m = \frac{\frac{m}{n}(e^\epsilon - 1) - \frac{1}{n}}{\left(\frac{m}{n} - \frac{1}{k}\right)(e^\epsilon - 1) - \frac{1}{n}} \tag{106}$$

$$= \frac{\frac{m}{n}(e^\epsilon - 1) - \frac{1}{n} - \frac{1}{k}(e^\epsilon - 1) + \frac{1}{k}(e^\epsilon - 1)}{\left(\frac{m}{n} - \frac{1}{k}\right)(e^\epsilon - 1) - \frac{1}{n}} \tag{107}$$

$$= \frac{\left(\frac{m}{n} - \frac{1}{k}\right)(e^\epsilon - 1) - \frac{1}{n} + \frac{1}{k}(e^\epsilon - 1)}{\left(\frac{m}{n} - \frac{1}{k}\right)(e^\epsilon - 1) - \frac{1}{n}} \tag{108}$$

$$= 1 + \frac{\frac{1}{k}(e^\epsilon - 1)}{\left(\frac{m}{n} - \frac{1}{k}\right)(e^\epsilon - 1) - \frac{1}{n}} \tag{109}$$

$$= 1 - \frac{\frac{1}{k}(e^\epsilon - 1)}{\left(\frac{1}{k} - \frac{m}{n}\right)(e^\epsilon - 1) + \frac{1}{n}}. \tag{110}$$

As  $m$  increases, (110) becomes smaller due to a larger fraction being subtracted from 1. Thus,  $t_m$  is decreasing in  $m$ . Now, we prove the lemma for the base case and apply induction.

*Base case:* For  $m = 1$ , we have

$$q_1 = \frac{u_1}{v_1} q_0 - \frac{w_1}{v_1} \tag{111}$$

$$= \frac{u_1}{v_1} t_0 - \left(\frac{u_1}{v_1} - 1\right) t_1 \tag{112}$$

$$= \frac{u_1}{v_1} (t_0 - t_1) + t_1 \tag{113}$$

$$> t_1, \tag{114}$$

since  $\frac{u_1}{v_1} > 0$ , and  $t_m$  is strictly decreasing in  $m$ .

*Induction step:* Let us assume  $q_m > t_m$  for any  $m$ . We have

$$q_{m+1} = \frac{u_{m+1}}{v_{m+1}} q_m - \frac{w_{m+1}}{v_{m+1}} \quad (115)$$

$$= \frac{u_{m+1}}{v_{m+1}} q_m - \left( \frac{u_{m+1}}{v_{m+1}} \right) t_{m+1} \quad (116)$$

$$> \frac{u_{m+1}}{v_{m+1}} t_m - \left( \frac{u_{m+1}}{v_{m+1}} \right) t_{m+1} \quad (117)$$

$$= \frac{u_{m+1}}{v_{m+1}} (t_m - t_{m+1}) + t_{m+1} \quad (118)$$

$$> t_{m+1}. \quad (119)$$

Thus, for  $m = 1, 2, \dots, \left\lfloor \frac{1}{e^\epsilon - 1} \right\rfloor$ ,  $q_m$  satisfies (102). ■

#### ACKNOWLEDGMENT

This work is supported in part by NSF grants CIF-1901243, CIF-2312666, and CIF-2007688.

#### REFERENCES

- [1] C. Dwork, F. McSherry, K. Nissim, and A. Smith, “Calibrating noise to sensitivity in private data analysis,” in *Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006. Proceedings 3*. Springer, 2006, pp. 265–284.
- [2] C. Dwork, A. Roth *et al.*, “The algorithmic foundations of differential privacy,” *Foundations and Trends® in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2014.
- [3] G. Kamath, J. Li, V. Singhal, and J. Ullman, “Privately learning high-dimensional distributions,” in *Conference on Learning Theory*. PMLR, 2019, pp. 1853–1902.
- [4] S. Raskhodnikova, S. Sivakumar, A. Smith, and M. Swanberg, “Differentially private sampling from distributions,” *Advances in Neural Information Processing Systems*, vol. 34, pp. 28 983–28 994, 2021.
- [5] B. Ghazi, X. Hu, R. Kumar, and P. Manurangsi, “On differentially private sampling from gaussian and product distributions,” *Advances in Neural Information Processing Systems*, vol. 36, 2024.
- [6] H. Husain, B. Balle, Z. Cranko, and R. Nock, “Local differential privacy for sampling,” in *International Conference on Artificial Intelligence and Statistics*. PMLR, 2020, pp. 3404–3413.
- [7] J. Acharya, C. L. Canonne, and H. Tyagi, “Inference under information constraints i: Lower bounds from chi-square contraction,” *IEEE Transactions on Information Theory*, vol. 66, no. 12, pp. 7835–7855, 2020.
- [8] —, “Inference under information constraints ii: Communication constraints and shared randomness,” *IEEE Transactions on Information Theory*, vol. 66, no. 12, pp. 7856–7877, 2020.
- [9] S. M. Bellovin, P. K. Dutta, and N. Reitinger, “Privacy and synthetic datasets,” *Stan. Tech. L. Rev.*, vol. 22, p. 1, 2019.
- [10] M. Hardt, K. Ligett, and F. McSherry, “A simple and practical algorithm for differentially private data release,” *Advances in neural information processing systems*, vol. 25, 2012.
- [11] T. Zhu, G. Li, W. Zhou, and S. Y. Philip, “Differentially private data publishing and analysis: A survey,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 29, no. 8, pp. 1619–1638, 2017.
- [12] A. Majeed and S. Lee, “Anonymization techniques for privacy preserving data publishing: A comprehensive survey,” *IEEE access*, vol. 9, pp. 8512–8545, 2020.
- [13] M. Boedihardjo, T. Strohmer, and R. Vershynin, “Private sampling: a noiseless approach for generating differentially private synthetic data,” *SIAM Journal on Mathematics of Data Science*, vol. 4, no. 3, pp. 1082–1115, 2022.
- [14] B. Axelrod, S. Garg, V. Sharan, and G. Valiant, “Sample amplification: Increasing dataset size even when learning is impossible,” in *International Conference on Machine Learning*. PMLR, 2020, pp. 442–451.