

An Improved Christofides Mechanism for Local Differential Privacy Framework

She Sun
AI Research Institute
Zhejiang Lab
Hangzhou, Zhejiang, China
sunshe@zhejianglab.com

Li Zhou
AI Research Institute
Zhejiang Lab
Hangzhou, Zhejiang, China
zhou.li@zhejianglab.com

Xiaoran Yan*
AI Research Institute
Zhejiang Lab
Hangzhou, Zhejiang, China
yanxr@zhejianglab.com

ABSTRACT

The development of Internet technology enables an analysis on the whole population rather than a certain number of samples, and leads to increasing requirement for privacy protection. Local differential privacy (LDP) is an effective standard of privacy measurement; however, its large variance of mean estimation causes challenges in application. To address this problem, this paper presents a new LDP approach, an improved Christofides mechanism.

It compared four statistical survey methods for conducting surveys on sensitive topics—modified Warner, Simmons, Christofides, and the improved Christofides mechanism. Specifically, Warner, Simmons and Christofides mechanisms have been modified to draw a sample from the population without replacement, to decrease variance. Furthermore, by drawing cards without replacement based on modified Christofides mechanism, we introduce a new mechanism called the improved Christofides mechanism, which is found to have the smallest variance under certain assumption when using LDP as a measurement of privacy leakage. The assumption is do satisfied usually in the real world. Actually, we decrease the variance to 28.7% of modified Christofides mechanism’s variance in our experiment based on the HCOVANY dataset—a real world dataset of IPUMS USA. This means our method gets a more accurate estimate by using LDP as a measurement of privacy leakage. This is the first time the improved Christofides mechanism is proposed for LDP framework based on comparative analysis of four mechanisms using LDP as the same measurement of privacy leakage.

PVLDB Reference Format:

She Sun, Li Zhou, and Xiaoran Yan. An Improved Christofides Mechanism for Local Differential Privacy Framework. PVLDB, 16(1): XXX-XXX, 2023. doi:XX.XX/XXX.XX

PVLDB Artifact Availability:

The source code, data, and/or other artifacts have been made available at URL_TO_YOUR_ARTIFACTS.

*Corresponding author: yanxr@zhejianglab.com.

This work is licensed under the Creative Commons BY-NC-ND 4.0 International License. Visit <https://creativecommons.org/licenses/by-nc-nd/4.0/> to view a copy of this license. For any use beyond those covered by this license, obtain permission by emailing info@vldb.org. Copyright is held by the owner/author(s). Publication rights licensed to the VLDB Endowment.

Proceedings of the VLDB Endowment, Vol. 16, No. 1 ISSN 2150-8097.
doi:XX.XX/XXX.XX

1 INTRODUCTION

Local differential privacy (LDP), proposed in [24] as the first equivalent definition and further developed by Duchi et al. [11], is an algorithm which quantifies privacy by having users randomly perturb their data locally and send the perturbed data to a (possibly un-trusted) data collector. Since the data collector does not hold the original personal data, it is a strong privacy model [3–5, 7, 9, 29, 30, 33, 34]. LDP has been adopted by many industry organizations, including Apple [26], Google [13], and Microsoft [10]. For instance, Apple [26] deploys LDP on iOS to know popular health data types for future improvement in the Health app. Google [13] has adopted RAPPOR to Chrome Web browser, collecting data about Chrome clients from approximately 14 million respondents who have opted to send usage statistics to Google. Microsoft [10] integrates LDP in Windows 10 to collect the number of seconds that a user has spent using a particular app.

In social science and epidemiologic research, surveying sensitive questions such as cheat, gamble, drug or alcohol abuse, or antisocial behavior, is likely to lead to refusals or untruthful answers. To address this issue, Warner et al. [31] proposed a procedure as randomized response, the most classical LDP mechanism, in 1965. Since then, many mechanisms [8, 14, 16–18, 21, 22] for surveying sensitive questions have been proposed, two iconic ones being [17] and [8]. Simmons et al. [17] suggested in 1967 that the level of cooperation would increase if two unrelated questions (or statements) were used. Christofides et al. [8] proposed a generalization randomized response technique in 2003, where users only have to answer with numbers instead of *yes* or *no*.

Waseda et al. [32] evaluated Warner, Kuk [18], negative survey mechanism [14] and its variants [2] by using differential privacy. They showed that these mechanisms have a tradeoff between privacy and utility, but did not compare the performance of different mechanisms nor suggest ways to improve them. Giordano et al. [15] compared the variance of the estimators of three dichotomous unrelated question mechanisms ([17, 23, 25]) under equal levels of confidentiality measures introduced by Lanke [19], Leysieffer and Warner [20], but also did not improve the performance of variance.

With the development of big data and artificial intelligence, people can collect data not by sampling, but by surveying the population, such as in U.S. Census 2020 and the US presidential election of 2020. And with that in mind, we modified three mechanisms (Warner, Simmons and Christofides mechanisms) for conducting surveys on sensitive topics by drawing a sample from the population without replacement. Since drawing a sample from the population without replacement can reduce the randomness of the

estimated mean in our case, we improved modified Christofides mechanism by drawing cards from device without replacement. The improvement is remarkable for the variance of the improved Christofides mechanism is the smallest when the proportion of people with sensitive attributes is small if we use LDP as the same measurement of privacy leakage. In fact, the variance decreases to 28.7% that of modified Christofides mechanism in our experiment base on a read world dataset. As a result, we find a new LDP mechanism for mean estimation with smaller variance and a better degree of cooperation from data providers.

Contributions. Our contributions are threefold:

(1) We analyze modified Warner, Simmons and Christofides mechanisms by drawing samples from the population without replacement.

(2) We propose an improved Christofides mechanism with a small but effective change to modified Christofides mechanism when the proportion of people with sensitive attributes is small.

(3) We compare the variance of modified Warner, Simmons, Christofides and the improved Christofides mechanisms by theoretical analysis and numerical simulation using LDP as the same measurement of privacy leakage. We find that the improved Christofides mechanisms has the smallest variance when the proportion of people with sensitive attributes is small, and can be used as a better LDP mechanism to replace Warner mechanism.

Organization. Section 2 presents the background, including the definition of LDP and the procedures of Warner, Simmons and Christofides mechanisms. Section 3 presents the procedures and variances of modified Warner, and Simmons and Christofides mechanisms by theoretical analysis. In section 4, we introduce the improved Christofides mechanism and analyze its variance. In section 5, we analyze the variance of modified Warner, Simmons and Christofides and the improved Christofides mechanism by using LDP as the measurement of privacy leakage. In section 6, we compare the variance and minimum sample size of four mechanisms by theoretical analysis and numerical simulation. In section 7, we give the conclusion.

2 BACKGROUND

2.1 Local Differential Privacy

In the LDP setting, a user perturbs the private value x using an algorithm $\mathcal{A}$ and sends $\mathcal{A}(x)$ to the untrusted collector. The collector learns statistical information about users.

Definition 2.1 (ϵ -LDP [11]). A randomization mechanism $\mathcal{A}$ satisfies ϵ -LDP, if and only if for any pair of input values x, x' and for all randomized output O , it holds that

$$\mathbf{P}[\mathcal{A}(x) = O] \leq e^\epsilon \times \mathbf{P}[\mathcal{A}(x') = O].$$

The notation $\mathbf{P}$ means probability.

2.2 Three Randomized Response Mechanisms

This section briefly introduces Warner Mechanism, Simmons mechanism and Christofides mechanism.

2.2.1 Warner Mechanism [31]. Suppose that each respondent in a population belongs to either Group A or $\bar{A}$ and that it is required

to estimate the proportion of Group A by survey. Each respondent is required to respond *yes* or *no* to one of the two statements:

- (a) I am a member of group A .
- (b) I am a member of group $\bar{A}$.

The respondent responds to statement (a) with probability p ($p < 1/2$ in this paper.) and to statement (b) with probability $1 - p$ using a random device, e.g., by the toss of a (biased) coin and in the absence of the interviewer. The investigator, such as the government or school, can get the unbiased estimate of the true proportion of people with sensitive attributes according to the answers.

2.2.2 Simmons Mechanism [17]. It is noted that both statements of Warner mechanism are sensitive. In Simmons mechanism, we change the second statement of Warner mechanism to an unrelated one, which leads to a higher degree of cooperation for the respondent compared with that of Warner mechanism.

Simmons mechanism uses two statements:

- (a) I am a member of Group A .
- (b) I am a member of Group B .

, where the unrelated statement in Group B is unsensitive. For instance, the two statements posed might be:

- (a) I cheated in an exam.
- (b) I was born in the first half of the year.

The investigator, such as the government or school, can get the unbiased estimator of the true proportion of people with sensitive attributes according to the answers.

2.2.3 Christofides Mechanism [8]. In Christofides mechanism, every respondent is provided with a card which produces the integers $1, 2, \dots, L$ with proportions $p_1, p_2, \dots, p_L$ respectively (These proportions are not all equal). The respondent reports how far away the integer is from $L + 1$ if he/she has the sensitive attributes or from 0 if he/she does not have it. For instance, suppose that L is 3 and the respondent reports the number 3. This means that either the respondent has sensitive attributes and the drawn number is 1 or the respondent does not have sensitive attributes and the drawn number is 3. Notice that when $L = 2$, Christofides mechanism is substantially equivalent to Warner mechanism.

The investigator, such as the government or school, can get the unbiased estimate of the true proportion of people with sensitive attributes according to the answers.

3 ANALYZING THREE MODIFIED MECHANISMS

This section analyzes modified Warner, Simmons and Christofides mechanisms. We assume the whole procedure is completed by the respondent and unobserved by the investigator with all respondents being truthful in their answers.

In [31] [17] and [8], the authors assumed a random sampling from the population with replacement. However, due to the development of the Internet, people can let the number of samples and populations be equal, such as in U.S. Census 2020 [6] and the US presidential election, which means sampling without replacement.

Let x_i be the integer representing the sensitive attributes of respondent i , which is 1 if the respondent is a member of sensitive group (persons with no health insurance coverage at the time of interview), and 0 if the respondent is not a member of sensitive group

(persons with health insurance coverage at the time of interview in our experiment). We have

$$x_i = \begin{cases} 1, & \text{respondent } i \in \text{Group } A \\ 0, & \text{respondent } i \in \text{Group } \bar{A}. \end{cases}$$

3.1 Analyzing Modified Warner Mechanism

Algorithm 1 illustrates modified Warner Mechanism. We select from the population of size N a random sample without replacement of size N . Let π_A be the true proportion of being a member of group A in the population.

Algorithm 1 modified Warner Mechanism

Input: $x_i (i = 1, 2, \dots, N), p$

Output: X_i

- 1: Sample a Bernoulli variable u such that $P(u = 1) = p$
 - 2: **if** $u < p$ **then**
 - 3: $X_i = x_i$
 - 4: **else**
 - 5: $X_i = 1 - x_i$
 - 6: **end if**
 - 7: **return** X_i
 - 8: Experiment with the next respondent $i + 1$.
-

Introduce random variables

$$X_i = \begin{cases} 1, & \text{the } i \text{ th respondent answers yes} \\ 0, & \text{the } i \text{ th respondent answers no.} \end{cases}$$

Random variables $X_1, X_2, \dots, X_N$ are dependent. The number of yes answers obtained from N respondents is $N_1 = \sum_{i=1}^N X_i$.

According to the formula of total probability, the theoretical proportion of the respondent who answered yes to question (a) or (b) is approximately equal to N_1/N , shown as follows,

$$p\pi_A + (1-p)(1-\pi_A) \approx \frac{N_1}{N}.$$

The parameter π_A is estimated based on the indirect responses of all respondents via the estimator

$$\hat{\pi}_A = \frac{\frac{N_1}{N} - (1-p)}{2p-1}.$$

The estimator $\hat{\pi}_A$ is unbiased estimation according to the Law of large numbers [12].

The variance of $\hat{\pi}_A$ [28] is

$$\begin{aligned} \text{Var}\hat{\pi}_A &= \frac{\text{Var}(\sum_{i=1}^N X_i)}{N^2(2p-1)^2} \\ &= \frac{\pi_A p(1-p) + (1-\pi_A)(1-p)p}{N(2p-1)^2} \\ &= \frac{p(1-p)}{N(2p-1)^2}. \end{aligned} \quad (1)$$

The variance is decreased by $[\pi_A(1-\pi_A)]/N$ compared with that in [31] that samples with replacement, which is

$$\text{Var}\hat{\pi}_A = \frac{\pi_A(1-\pi_A)}{N} + \frac{p(1-p)}{N(2p-1)^2}.$$

3.2 Analyzing Modified Simmons Mechanism

Algorithm 2 illustrates modified Simmons Mechanism. We select from the population of size N a random sample without replacement of size N . Let π_A be the true proportion of being a member of group A in the population.

Algorithm 2 modified Simmons Mechanism

Input: $x_i (i = 1, 2, \dots, N), p, \pi_B$

Output: X_i

- 1: Sample a Bernoulli variable u such that $P(u = 1) = p$
 - 2: **if** $u < p$ **then**
 - 3: $X_i = x_i$
 - 4: **else**
 - 5: Sample a Bernoulli variable v such that $P(v = 1) = \pi_B$
 - 6: **if** $v < \pi_B$ **then**
 - 7: $X_i = 1$
 - 8: **else**
 - 9: $X_i = 0$
 - 10: **end if**
 - 11: **end if**
 - 12: **return** X_i
 - 13: Experiment with the next respondent $i + 1$.
-

Introduce random variables

$$X_i = \begin{cases} 1, & \text{the } i \text{ th respondent answers yes} \\ 0, & \text{the } i \text{ th respondent answers no.} \end{cases}$$

Random variables $X_1, X_2, \dots, X_N$ are dependent. The number of yes answers obtained from N respondents is $N_1 = \sum_{i=1}^N X_i$.

According to the formula of total probability, the theoretical proportion of the respondent who answered yes to question (a) or (b) is approximately equal to N_1/N , shown as follows,

$$p\pi_A + (1-p)\pi_B \approx \frac{N_1}{N}.$$

The parameter π_A is estimated based on the indirect responses of all respondents via the estimator

$$\hat{\pi}_A = \frac{\frac{N_1}{N} - (1-p)\pi_B}{p}.$$

The estimator $\hat{\pi}_A$ is an unbiased estimation according to the Law of large numbers [12].

The variance of $\hat{\pi}_A$ is

$$\begin{aligned} \text{Var}\hat{\pi}_A &= \frac{\text{Var}\left(\frac{1}{N} \sum_{i=1}^N X_i\right)}{p^2} \\ &= \frac{\pi_A [p + (1-p)\pi_B] [1-p - (1-p)\pi_B]}{Np^2} + \\ &\quad \frac{(1-\pi_A) [(1-p)\pi_B] [1 - (1-p)\pi_B]}{Np^2} \\ &= \frac{\pi_B(1-p) - \pi_B^2(1-p)^2}{Np^2} + \\ &\quad \pi_A \frac{1-p - 2\pi_B(1-p)}{Np}. \end{aligned} \quad (2)$$

The variance is decreased by $[\pi_A(1 - \pi_A)]/N$ compared with that in [17] which samples with replacement,

$$\text{Var}\hat{\pi}_A = \frac{\pi_A(1 - \pi_A)}{N} + \frac{\pi_B(1 - p) - \pi_B^2(1 - p)^2}{Np^2} + \pi_A \frac{1 - p - 2\pi_B(1 - p)}{Np}.$$

3.3 Analyzing Modified Christofides Mechanism

Algorithm 3 illustrates modified Christofides Mechanism. We draw a sample of size N from the population of size N without replacement. To formulate the algorithm mathematically, prepare M cards, which produce integers $1, 2, \dots, L$ with proportions $p_1, p_2, \dots, p_L$ respectively (These proportions are not all equal). Let π_A be the true proportion of being a member of group A in the population.

Algorithm 3 modified Christofides Mechanism

Input: $x_i (i = 1, 2, \dots, N), L, p_1, p_2, \dots, p_L$

Output: X_i

- 1: prepare a device consist of M cards, each card showing one of the integers $1, 2, \dots, L$ with proportions $p_1, p_2, \dots, p_L$ respectively;
 - 2: randomly select a card, assume the number is k ;
 - 3: **if** $x_i = 1$ **then**
 - 4: $X_i = k$;
 - 5: **else**
 - 6: $X_i = L + 1 - k$
 - 7: **end if**
 - 8: return X_i ;
 - 9: Put the card back to device.
 - 10: Experiment with the next respondent $i + 1$.
-

For convenience, we introduce the following notations: Y_i is the number he/she draws and X_i is the number he/she answers.

We have

$$X_i = \begin{cases} 1, & \text{the } i \text{ th respondent answers yes} \\ 0, & \text{the } i \text{ th respondent answers no} \end{cases}$$

, where

$$X_i = (L + 1 - Y_i) x_i + Y_i (1 - x_i).$$

The expectation of X is

$$EX = EY + \pi(L + 1 - 2EY).$$

Thus the estimation of π_A is

$$\hat{\pi}_A = \frac{\frac{1}{N} \sum_{i=1}^N X_i - E(Y)}{L + 1 - 2E(Y)}.$$

The estimator $\hat{\pi}_A$ is an unbiased estimation according to the Law of large numbers [12].

THEOREM 3.1 (MODIFIED CHRISTOFIDES MECHANISM VARIANCE).
The variance of $\hat{\pi}_A$ is

$$\begin{aligned} \text{Var}\hat{\pi}_A &= \frac{\text{Var}\left(\sum_{i=1}^N X_i\right)}{N^2(L + 1 - 2E(Y))^2} \\ &= \frac{\text{Var}Y}{N(L + 1 - 2E(Y))^2}. \end{aligned}$$

PROOF. The proof is in Appendix A. □

The variance is decreased by $[\pi_A(1 - \pi_A)]/N$ compared with that in [8] which samples with replacement,

$$\text{Var}\hat{\pi}_A = \frac{\pi_A(1 - \pi_A)}{N} + \frac{\text{Var}Y}{N(L + 1 - 2E(Y))^2}.$$

By modifying Warner, Simmons and Christofides by sampling without replacement, the variance is decreased by $[\pi_A(1 - \pi_A)]/N$ compared with that in [31] [17] and [8], which samples with replacement. This is our first contribution.

4 THE IMPROVED CHRISTOFIDES MECHANISM

Since drawing a random sample from the population without replacement can reduce the randomness of the estimated mean in our case. What will happen if respondent draws cards without replacement? To clarify this issue, we proposed the improved Christofides mechanism, which is illustrated as Algorithm 4.

Algorithm 4 the improved Christofides Mechanism

Input: $x_i (i = 1, 2, \dots, N), L, p_1, p_2, \dots, p_L$

Output: X_i

- 1: prepare a device consist of N cards, each card showing one of the integers $1, 2, \dots, L$ with proportions $p_1, p_2, \dots, p_L$ respectively;
 - 2: randomly select a card, assume the number is k ;
 - 3: **if** $x_i = 1$ **then**
 - 4: $X_i = k$;
 - 5: **else**
 - 6: $X_i = L + 1 - k$
 - 7: **end if**
 - 8: return X_i ;
 - 9: The respondent keeps the card. (Do not put the card back to device.)
 - 10: Experiment with the next respondent $i + 1$.
-

We select from the population of size N a sample without replacement of size N . To formulate the algorithm mathematically, prepare N cards, which produce integers $1, 2, \dots, L$ with proportions $p_1, p_2, \dots, p_L$ respectively (These proportions are not all equal).

For convenience, we introduce the following notations: Y_i is the number he/she draws and X_i is the number he/she answers.

We have

$$X_i = \begin{cases} 1, & \text{the } i \text{ th respondent answers yes} \\ 0, & \text{the } i \text{ th respondent answers no,} \end{cases}$$

where

$$X_i = (L + 1 - Y_i) x_i + Y_i (1 - x_i).$$

The expectation of X is

$$EX = EY + \pi(L + 1 - 2EY).$$

Thus the estimation of π_A is

$$\hat{\pi}_A = \frac{\frac{1}{N} \sum_{i=1}^N X_i - E(Y)}{L + 1 - 2E(Y)}.$$

The estimator $\hat{\pi}_A$ is an unbiased estimation according to the Law of large numbers [12].

THEOREM 4.1 (THE IMPROVED CHRISTOFIDES MECHANISM VARIANCE). *The variance of $\hat{\pi}_A$ is*

$$\begin{aligned} \text{Var}\hat{\pi}_A &= \frac{\text{Var}\left(\sum_{i=1}^N X_i\right)}{N^2(L + 1 - 2E(Y))^2} \\ &= \frac{4\pi_A(1 - \pi_A)\text{Var}(Y)}{(N - 1)(L + 1 - 2E(Y))^2}. \end{aligned} \quad (3)$$

PROOF. *The proof is in Appendix B.* $\square$

Since the estimation of π_A for modified Christofides mechanisms and the improved Christofides mechanism are all unbiased estimations, we compare the utility of the two mechanisms by calculating the difference between the variance of modified Christofides (Var_{IC}) and the improved Christofides mechanism (Var_{MC}).

THEOREM 4.2 (COMPARISON MODIFIED CHRISTOFIDES AND THE IMPROVED CHRISTOFIDES MECHANISMS BY THEORETICAL ANALYSIS). *The comparison can be summarized as follows:*

- (i.) *When proportion π_A is in interval $(0, 1/2 - 1/2\sqrt{N}) \cup (1/2 + 1/2\sqrt{N}, 1)$, we get that Var_{IC} is smaller than Var_{MC} .*
- (ii.) *When proportion π_A is in interval $(1/2 - 1/2\sqrt{N}, 1/2 + 1/2\sqrt{N})$, we get that Var_{IC} is larger than Var_{MC} .*

PROOF.

$$\begin{aligned} &\text{Var}_{IC}\hat{\pi}_A - \text{Var}_{MC}\hat{\pi}_A \\ &= \left[\frac{4\pi_A(1 - \pi_A)}{N - 1} - \frac{1}{N} \right] \frac{\text{Var}Y}{(L + 1 - 2EY)^2} \\ &= \left[\frac{-4N\pi_A^2 + 4N\pi_A - N + 1}{N(N - 1)} \right] \frac{\text{Var}Y}{(L + 1 - 2EY)^2} \\ &= -\frac{4(1/2 + 1/2\sqrt{N} - \pi_A)(1/2 - 1/2\sqrt{N} - \pi_A)\text{Var}Y}{(N - 1)(L + 1 - 2EY)^2}. \end{aligned}$$

As long as $\pi_A < 1/2 - 1/2\sqrt{N}$ or $\pi_A > 1/2 + 1/2\sqrt{N}$, we have

$$\text{Var}_{IC}\hat{\pi}_A < \text{Var}_{MC}\hat{\pi}_A. \quad \square$$

Because N is a large number, the interval $[1/2 - 1/2\sqrt{N}, 1/2 + 1/2\sqrt{N}]$ is small. For example, when $N = 10^4$, the interval is $[0.495, 0.505]$. Especially, since $1/2\sqrt{N} \leq 1/4$ (for $N \geq 3$), as long as $\pi_A < 0.25$ or $\pi_A > 0.75$, we have $\text{Var}_{IC} < \text{Var}_{MC}$ for any N ($N > 3$).

Moreover, we will prove in section 6 that the variance of the improved Christofides mechanism is smaller than that of modified Warner and Simmons mechanisms under certain assumption, in using LDP as a measurement of privacy leakage. The assumption

is do satisfied usually in the real world. We improved Christofides mechanism by sampling cards without replacement. This is our second contribution.

5 ANALYZING FOUR MECHANISMS VARIANCES USING LDP

In this section, we analyzed the variance of four mechanisms by theoretical analysis using LDP as the same measurement of privacy leakage.

5.1 Modified Warner Mechanism using LDP

THEOREM 5.1 (WARNER MECHANISM). *Modified Warner mechanism satisfies ϵ -differential privacy, where $\epsilon = \ln[(1 - p)/p]$ (without losing of generality, suppose that $p < 1/2$).*

PROOF. We consider four cases:

Case 1: The respondent has sensitive attributes, and the probability of answering *yes* under this condition is p .

Case 2: The respondent has sensitive attributes, and the probability of answering *no* under this condition is $1 - p$.

Case 3: The respondent does not have sensitive attributes, and the probability of answering *yes* under this condition is $1 - p$.

Case 4: The respondent does not have sensitive attributes, and the probability of answering *no* under this condition is p .

For any two respondents with the same answer, the maximum ratio of proportions is $(1 - p)/p$. $\square$

Substitute $\epsilon = \ln[(1 - p)/p]$ and $p < 1/2$ into equation (1). The variance Var_{MW} can be written as

$$\text{Var}\hat{\pi}_A = \frac{e^\epsilon}{N(e^\epsilon - 1)^2}.$$

5.2 Modified Simmons Mechanism using LDP

THEOREM 5.2 (SIMMONS MECHANISM). *Modified Simmons mechanism satisfies ϵ -differential privacy, where*

$$\epsilon = \begin{cases} \ln \frac{p+(1-p)\pi_B}{(1-p)\pi_B} & , \pi_B \leq \frac{1}{2} \\ \ln \frac{p+(1-p)(1-\pi_B)}{(1-p)(1-\pi_B)} & , \pi_B > \frac{1}{2}. \end{cases} \quad (4)$$

PROOF. We consider four cases:

Case 1: The respondent has sensitive attributes, and the probability of answering *yes* under this condition is $p + (1 - p)\pi_B$.

Case 2: The respondent has sensitive attributes, and the probability of answering *no* under this condition is $(1 - p)(1 - \pi_B)$.

Case 3: The respondent does not have sensitive attributes, and the probability of answering *yes* under this condition is $(1 - p)\pi_B$.

Case 4: The respondent does not have sensitive attributes, and the probability of answering *no* under this condition is $p + (1 - p)(1 - \pi_B)$.

For any two respondents with the same answer, the maximum ratio of proportions is

$$\epsilon = \begin{cases} \ln \frac{p+(1-p)\pi_B}{(1-p)\pi_B} & , \pi_B \leq \frac{1}{2} \\ \ln \frac{p+(1-p)(1-\pi_B)}{(1-p)(1-\pi_B)} & , \pi_B > \frac{1}{2}. \end{cases} \quad \square$$

THEOREM 5.3 (MODIFIED SIMMONS MECHANISM VARIANCE VERSUS EPSILON). When $\pi_B = 1/2$, the variance Var_{MS} obtains its minimum as following

$$\text{Var}\hat{\pi}_A = \frac{e^\epsilon}{N(e^\epsilon - 1)^2}.$$

which is the same with that of modified Warner mechanism.

PROOF. The proof is in Appendix C. $\square$

5.3 Modified Christofides Mechanism using LDP

THEOREM 5.4 (MODIFIED CHRISTOFIDES MECHANISM). Modified Christofides mechanism satisfies ϵ -differential privacy, where

$$\epsilon = \max \left(\ln \frac{p_{L+1-k}}{p_k}, k = 1, 2, \dots, L \right).$$

PROOF. We consider four cases:

Case 1: The respondent has sensitive attributes and draws k . The probability of answering $L+1-k$ under this condition is p_k .

Case 2: The respondent has sensitive attributes and draws $L+1-k$. The probability of answering k under this condition is p_{L+1-k} .

Case 3: The respondent does not have sensitive attributes and draws k . The probability of answering k under this condition is p_k .

Case 4: The respondent does not have sensitive attributes and draws $L+1-k$. The probability of answering $L+1-k$ under this condition is p_{L+1-k} .

For any two respondents with the same answer, the maximum ratio of probabilities is

$$\epsilon = \max \left(\ln \frac{p_{L+1-k}}{p_k}, k = 1, 2, \dots, L \right).$$

$\square$

We fix number $L = 3$, so the privacy budget ϵ is

$$\epsilon = \max \left\{ \ln \frac{p_1}{p_3}, \ln \frac{p_3}{p_1} \right\}.$$

THEOREM 5.5 (MODIFIED CHRISTOFIDES MECHANISM VARIANCE VERSUS EPSILON). For the case $L = 3$, the variance of the modified Christofides mechanism Var_{MC} arrives its minimum

$$\text{Var}\hat{\pi}_A = \frac{1}{4N} \left[\frac{(e^\epsilon + 1)^2}{(e^\epsilon - 1)^2 (1 - p_2)} - 1 \right].$$

under the situation that proportions

$$p_1 = (1 - p_2) / (e^\epsilon + 1), p_3 = [e^\epsilon (1 - p_2)] / (e^\epsilon + 1)$$

or

$$p_1 = [e^\epsilon (1 - p_2)] / (e^\epsilon + 1), p_3 = (1 - p_2) / (e^\epsilon + 1).$$

PROOF. The proof is in Appendix D. $\square$

Notice that when proportion $p_2 = 0$, modified Christofides mechanism is substantially equivalent to modified Warner mechanism.

5.4 Improved Christofides Mechanism using LDP

THEOREM 5.6 (THE IMPROVED CHRISTOFIDES MECHANISM). Suppose that any respondent does not know the cards others drew and the numbers others answered. Then the improved Christofides mechanism satisfies ϵ -differential privacy, where

$$\epsilon = \max \left(\ln \frac{p_{L+1-k}}{p_k}, k = 1, 2, \dots, L \right).$$

PROOF. We consider four cases:

Case 1: The respondent has sensitive attributes and draws k . The probability of answering $L+1-k$ under this condition is p_k .

Case 2: The respondent has sensitive attributes and draws $L+1-k$. The probability of answering k under this condition is p_{L+1-k} .

Case 3: The respondent does not have sensitive attributes and draws k . The probability of answering k under this condition is p_k .

Case 4: The respondent does not have sensitive attributes and draws $L+1-k$. The probability of answering $L+1-k$ under this condition is p_{L+1-k} .

For any two respondents with the same answer, the maximum ratio of probabilities is

$$\epsilon = \max \left(\ln \frac{p_{L+1-k}}{p_k}, k = 1, 2, \dots, L \right).$$

$\square$

We fix number $L = 3$, so the privacy budget ϵ is

$$\epsilon = \max \left\{ \ln \frac{p_1}{p_3}, \ln \frac{p_3}{p_1} \right\}.$$

THEOREM 5.7 (THE IMPROVED CHRISTOFIDES VARIANCE VERSUS EPSILON). For the case $L = 3$, the variance of the improved Christofides mechanism Var_{IC} arrives its minimum

$$\text{Var}\hat{\pi}_A = \frac{\pi_A (1 - \pi_A)}{(N - 1)} \left[\frac{(e^\epsilon + 1)^2}{(e^\epsilon - 1)^2 (1 - p_2)} - 1 \right]$$

under the situation that proportions

$$p_1 = (1 - p_2) / (e^\epsilon + 1), p_3 = [e^\epsilon (1 - p_2)] / (e^\epsilon + 1)$$

or

$$p_1 = [e^\epsilon (1 - p_2)] / (e^\epsilon + 1), p_3 = (1 - p_2) / (e^\epsilon + 1).$$

PROOF. The proof is similar with that in Appendix D. $\square$

6 COMPARING FOUR MECHANISMS USING LDP

Since the estimation of π_A for modified Warner/Simmons, Christofides mechanisms and the improved Christofides mechanism are all unbiased estimations, we compare variance of the four mechanisms by theoretical analysis and numerical simulation.

6.1 Comparing four Mechanisms using LDP by Theoretical Analysis

This section compares the utility of these four mechanisms by calculating variances under the same privacy budget ϵ .

THEOREM 6.1 (COMPARISON FOUR MECHANISMS USING LDP BY THEORETICAL ANALYSIS). *The comparison can be summarized as follows:*

- (i.) When proportion π_A is in interval $(0, \pi_{A_1}) \cup (\pi_{A_2}, 1)$, $\text{Var}_{\text{IC}} < \text{Var}_{\text{MW/MS}} < \text{Var}_{\text{MC}}$. π_{A_1} and π_{A_2} are shown in equation (5).
- (ii.) When proportion π_A is in interval $(\pi_{A_1}, 1/2 - 1/2\sqrt{N}) \cup (1/2 + 1/2\sqrt{N}, \pi_{A_2})$, $\text{Var}_{\text{MW/MS}} < \text{Var}_{\text{IC}} < \text{Var}_{\text{MC}}$.
- (iii.) When proportion π_A is in interval $(1/2 - 1/2\sqrt{N}, 1/2 + 1/2\sqrt{N})$, $\text{Var}_{\text{MW/MS}} < \text{Var}_{\text{MC}} < \text{Var}_{\text{IC}}$.

PROOF. Firstly, according to theorem 4.2, when proportion π_A is in interval $(1/2 - 1/2\sqrt{N}, 1/2 + 1/2\sqrt{N})$, we have $\text{Var}_{\text{IC}} > \text{Var}_{\text{MC}}$, while $\text{Var}_{\text{IC}} < \text{Var}_{\text{MC}}$ when proportion π_A is in interval $(0, 1/2 - 1/2\sqrt{N}) \cup (1/2 + 1/2\sqrt{N}, 1)$.

Secondly, we compare the variance of modified Christofides mechanism Var_{MC} with that of modified Warner/Simmons mechanisms ($\text{Var}_{\text{MW/MS}}$).

Since

$$\begin{aligned} & \text{Var}_{\text{MC}}\hat{\pi}_A - \text{Var}_{\text{MW/MS}}\hat{\pi}_A \\ &= \frac{(e^\epsilon + 1)^2 p_2}{4N(e^\epsilon - 1)^2(1 - p_2)}, \\ & \geq 0. \end{aligned}$$

the variance of modified Christofides mechanism Var_{MC} is large than that of modified Warner/Simmons mechanisms $\text{Var}_{\text{MW/MS}}$.

Then, we compare the variance of the improved Christofides mechanism Var_{IC} with that of modified Warner/Simmons mechanisms $\text{Var}_{\text{MW/MS}}$. The difference between the variances of the improved Christofides mechanism and modified Warner/Simmons mechanisms is

$$\begin{aligned} & \text{Var}_{\text{IC}}\hat{\pi}_A - \text{Var}_{\text{MW/MS}}\hat{\pi}_A \\ &= \frac{\pi_A(1 - \pi_A)}{N - 1} \left[\frac{(e^\epsilon + 1)^2}{(e^\epsilon - 1)^2(1 - p_2)} - 1 \right] - \frac{e^\epsilon}{N(e^\epsilon - 1)^2} \\ &= \frac{[4e^\epsilon + (e^\epsilon - 1)^2 p_2] \pi_A(1 - \pi_A) - (N - 1)(1 - p_2)e^\epsilon}{N(N - 1)(e^\epsilon - 1)^2(1 - p_2)} \end{aligned}$$

Let

$$a = 4e^\epsilon + (e^\epsilon - 1)^2 p_2, c = (N - 1)(1 - p_2)e^\epsilon$$

We have

$$\begin{aligned} & \text{Var}_{\text{IC}}\hat{\pi}_A - \text{Var}_{\text{MW/MS}}\hat{\pi}_A \\ &= \frac{-a\pi_A^2 + a\pi_A - c}{N(N - 1)(e^\epsilon - 1)^2(1 - p_2)} \\ &= \frac{-a(\pi_A - \pi_{A_1})(\pi_A - \pi_{A_2})}{N(N - 1)(e^\epsilon - 1)^2(1 - p_2)} \end{aligned}$$

$$\pi_{A_1} = \frac{a - \sqrt{\Delta}}{2a}$$

$$\pi_{A_2} = \frac{a + \sqrt{\Delta}}{2a}$$

$$\Delta = a^2 - 4ac.$$

$$\begin{aligned} \pi_{A_1} &= \frac{1}{2} - \frac{1}{2} \sqrt{1 - \frac{4c}{a}} \\ &= \frac{1}{2} - \frac{1}{2} \sqrt{1 - \frac{4e^\epsilon(N - 1)(1 - p_2)}{N[4e^\epsilon + p_2(e^{2\epsilon} - 2e^\epsilon + 1)]}} \\ &= \frac{1}{2} - \frac{1}{2} \sqrt{1 - \frac{(N - 1)(1 - p_2)}{N[1 + \frac{p_2}{4}(e^\epsilon + \frac{1}{e^\epsilon} - 2)]}}. \end{aligned}$$

$$\begin{aligned} \pi_{A_2} &= \frac{1}{2} + \frac{1}{2} \sqrt{1 - \frac{4c}{a}} \\ &= \frac{1}{2} + \frac{1}{2} \sqrt{1 - \frac{4e^\epsilon(N - 1)(1 - p_2)}{N[4e^\epsilon + p_2(e^{2\epsilon} - 2e^\epsilon + 1)]}} \\ &= \frac{1}{2} + \frac{1}{2} \sqrt{1 - \frac{(N - 1)(1 - p_2)}{N[1 + \frac{p_2}{4}(e^\epsilon + \frac{1}{e^\epsilon} - 2)]}}. \end{aligned}$$

Let

$$d = e^\epsilon + \frac{1}{e^\epsilon} - 2.$$

So

$$\begin{aligned} \pi_{A_1} &= \frac{1}{2} - \frac{1}{2} \sqrt{1 - \frac{N - 1}{N} \cdot \frac{1 - p_2}{1 + \frac{p_2 d}{4}}} \\ \pi_{A_2} &= \frac{1}{2} + \frac{1}{2} \sqrt{1 - \frac{N - 1}{N} \cdot \frac{1 - p_2}{1 + \frac{p_2 d}{4}}}. \end{aligned} \tag{5}$$

As long as $\pi_A < \pi_{A_1}$ or $\pi_A > \pi_{A_2}$, we have

$$\text{Var}_{\text{IC}}\hat{\pi}_A - \text{Var}_{\text{MW/MS}}\hat{\pi}_A < 0. \quad \square$$

The improved Christofides mechanism performs worst in interval $[\pi_{A_1}, \pi_{A_2}]$. The interval $[\pi_{A_1}, \pi_{A_2}]$ depends on N, ϵ and p_2 . Because the interval is symmetric about 0.5, we calculate the interval length under different proportions p_2 and privacy budgets ϵ after fix $N = 10^4$. The results are reported in Table 1. The interval $[\pi_{A_1}, \pi_{A_2}]$ is usually small.

Table 1: The length of interval $[\pi_{A_1}, \pi_{A_2}]$ under different proportion p_2 and privacy budget ϵ .

$\epsilon \backslash p_2$	0.01	0.05	0.25	0.5
0.01	0.100	0.101	0.101	0.104
0.05	0.224	0.224	0.225	0.230

6.2 Comparing four Mechanisms using LDP by Numerical Simulation

To plot the curve of variance versus privacy budget ϵ by numerical simulation for four mechanisms, we fix sample size $N = 10^2$ and proportion $\pi_A = 0.1$ for four mechanisms, fix proportion $\pi_B = 0.5$ for modified Simmons mechanism, and proportion $p_2 = 0.5$ for modified Christofides and the improved Christofides mechanisms. Then experiment according to algorithm 1 to 4. We report the results averaging 10000 runs. The theoretical analysis and numerical simulation result of four mechanisms is shown in Fig.1. The theoretical analysis value is verified by numerical simulation value. It shows that for these four mechanisms, the larger the privacy budget ϵ is, the smaller the variance is.

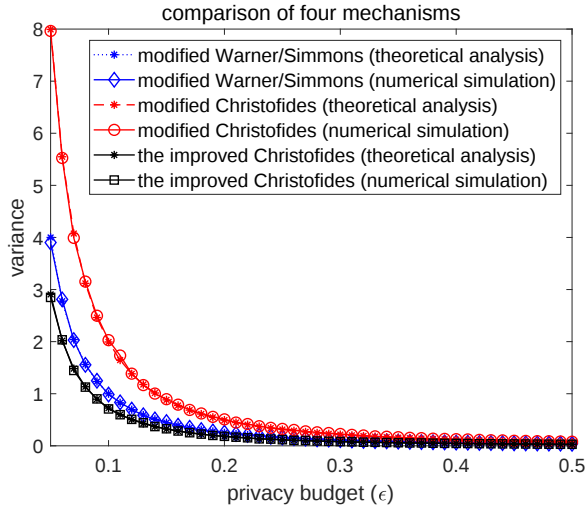


Figure 1: The variance versus privacy budget ϵ of four mechanisms when fix sample size $N = 10^2$ and proportion $\pi_A = 0.1$ (by theoretical analysis and numerical simulation).

We then report curves that variance versus privacy budget ϵ of four mechanisms by numerical simulation under different conditions in theorem 6.1. We fix sample size $N = 9$ for four mechanisms, fix proportions $\pi_B = 0.5$ for modified Simmons mechanism, fix proportion $p_2 = 0.36$ for modified Christofides and the improved Christofides mechanisms, and set proportion $\pi_A \in \{1/9, 2/9, 4/9\}$. The results are reported in Fig. 2 to 4.

Fig. 2 shows that when proportion π_A is in interval $(0, \pi_{A_1}) \cup (\pi_{A_2}, 1)$, the improved Christofides mechanism is the best, and modified Warner/Simmons mechanism is suboptimal, while modified Christofides mechanism is the worst.

Fig. 3 shows that when proportion π_A is in interval $(\pi_{A_1}, 1/2 - 1/2\sqrt{N}) \cup (1/2 + 1/2\sqrt{N}, \pi_{A_2})$, modified Warner/Simmons mechanism is the best, and the improved Christofides mechanism is suboptimal, while modified Christofides mechanism is the worst.

Fig. 4 shows that when proportion π_A is in interval $(1/2 - 1/2\sqrt{N}, 1/2 + 1/2\sqrt{N})$, modified Christofides mechanism is the best, and modified Warner/Simmons mechanism is suboptimal, while the improved Christofides mechanism is the worst.

In the real world, the proportion of people with sensitive attributes is usually small. This means the improved Christofides mechanism is usually the best method at most time.

Actually, in section 6.3, we experiment based on a real world dataset.

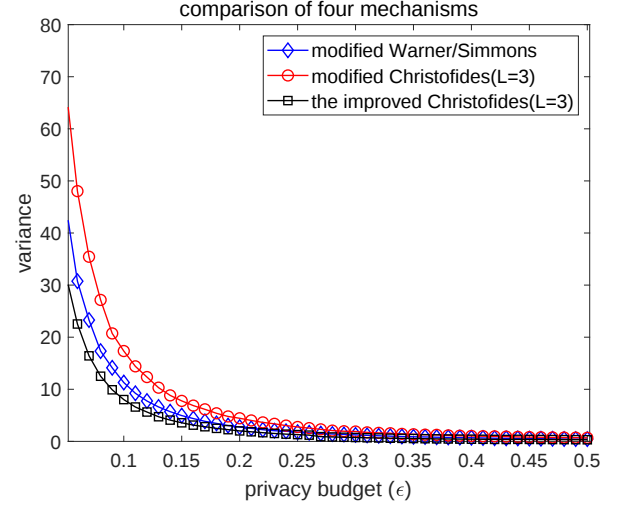


Figure 2: The variance versus privacy budget ϵ of four mechanisms when fix sample size $N = 9$ and proportion $\pi_A = 1/9$ (by numerical simulation).

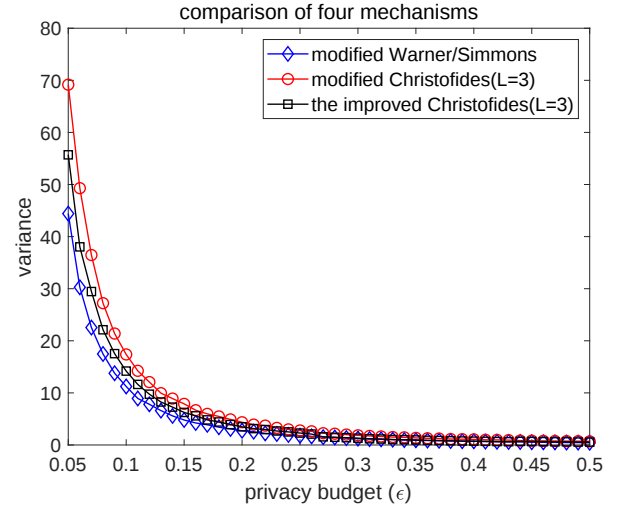


Figure 3: The variance versus privacy budget ϵ of four mechanisms when fix sample size $N = 9$ and proportion $\pi_A = 2/9$ (by numerical simulation).

6.3 Comparing four Mechanisms using LDP on a Real World Dataset

Dataset. HCOVANY Dataset [27]. We conduct our experiments on an open real world dataset. HCOVANY indicates whether persons

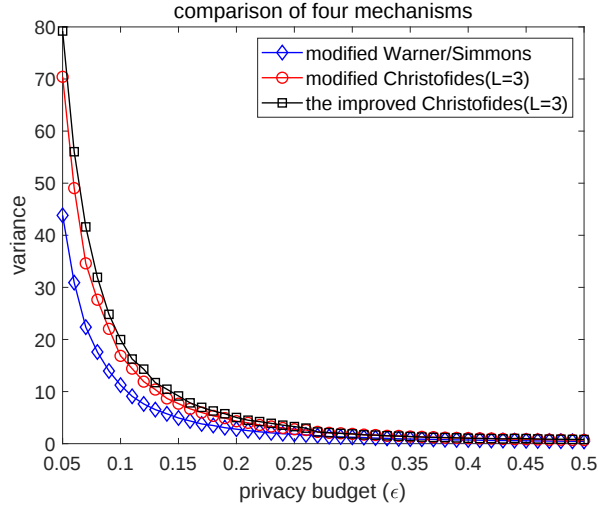


Figure 4: The variance versus privacy budget ϵ of four mechanisms when fix sample size $N = 9$ and proportion $\pi_A = 4/9$ (by numerical simulation).

had any health insurance coverage during the interview, as measured by employer-provided insurance (HINSEMP), privately purchased insurance (HINSPUR), Medicare (HINSCARE), Medicaid or other governmental insurance (HINSCAID), TRICARE or other military care (HINSTRI), or Veterans Administration-provided insurance (HINSVA). The Census Bureau does not consider the respondents with health insurance coverage if their only coverage is from Indian Health Services (HINSIHS), as IHS policies are not always comprehensive. Codes of 2 indicate that a person is covered (either directly or through another household member's policy) by the given type of insurance; codes of 1 indicate that a person is not covered. We select the subset of *HCOVANY Dataset* in our experiment (the health insurance coverage of 1% of total population in USA in 2021, the sampling size $N = 3252599$).

Privacy Budget ϵ . According to Harvard's list [1] of varying levels of sensitivity for datasets and reasonable privacy loss parameters for each level, we set privacy budget ϵ from 0.05 to 0.5, since health insurance coverage information that could cause risk of material harm to individuals if disclosed.

We fix proportion $p_2 = 0.01$ for modified Christofides mechanism and the improved Christofides mechanism. Then experiment according to algorithm 1 to 4. We report the results averaging 10^4 runs. The comparison of variance of these four mechanisms versus the privacy budget ϵ are shown in Fig. 5.

The variance of modified Warner mechanism is the same with that of modified Simmons mechanism. The variance of modified Christofides mechanism is slightly larger than that of modified Warner and Simmons mechanism. The variance of the improved Christofides mechanism is the smallest of mechanisms. In fact, we decrease the variance to 28.7% of modified Christofides mechanism's variance based on HCOVANY dataset.

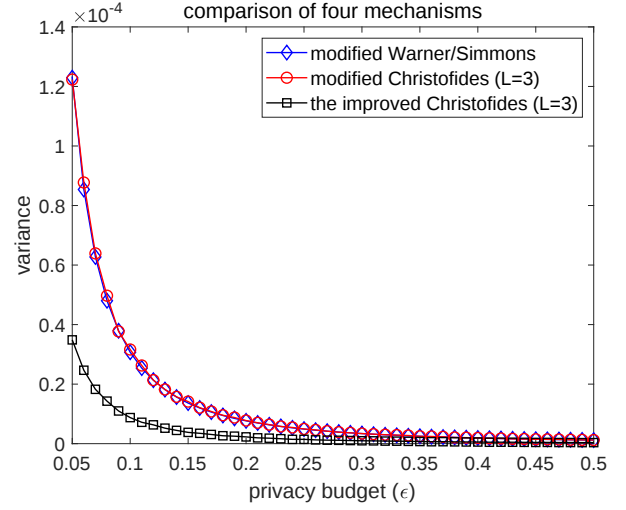


Figure 5: The comparison of variance versus privacy budget ϵ of four mechanisms based on HCOVANY dataset.

$$\begin{aligned} \frac{\text{Var}_{IC}\hat{\pi}_A}{\text{Var}_{MC}\hat{\pi}_A} &= \frac{4N\pi_A(1-\pi_A)}{N-1} \\ &= \frac{4 \times 3252599 \times 0.0778 \times (1 - 0.0778)}{3252599 - 1} \\ &= 28.7\%. \end{aligned}$$

6.4 Comparing the Minimum Sample Size of the four Mechanisms

Since an important task for statisticians is to determine the minimum number of samples N under given constraints, we compare the minimum sampling size N for the given proportion $\pi_A = 0.1$, variance $\text{Var}\hat{\pi}_A = 0.1$ and privacy budget ϵ of four mechanisms(modified Warner, Simmons, Christofides ($p_2 = 0.01$) and the improved Christofides mechanisms ($p_2 = 0.01$)). The result is shown in Table 2. The result shows that the larger the privacy budget ϵ is, the smaller the sample size N is for the four mechanisms. The minimum number of samples N of modified Warner and Simmons mechanisms are the same. The minimum number of samples N of modified Christofides mechanism is slightly larger than that of modified Warner/Simmons mechanisms. The minimum number of samples N of the improved Christofides mechanism is the smallest one.

Table 2: The minimum sampling size N for given proportion $\pi_A = 0.1$, variance $\text{Var}\hat{\pi}_A = 0.1$ and privacy budget ϵ of four mechanisms.

Mechanisms	Privacy Budget			
	0.01	0.05	0.25	0.5
modified Warner/Simmons	100000	4000	160	40
modified Christofides	101011	4040	161	40
the improved Christofides	36365	1456	59	16

Especially, if we do not know that the proportion belongs to sensitive group when using the improved Christofides mechanism, for example, under constraints of variance $\text{Var} \leq 0.1$, privacy budget $\varepsilon = 0.01$ and choosing proportion $p_2 = 0.01$, since the variance get the maximum when $\pi_A = 0.5$, sample size N should be at least 101011 ($N > 101010.3$).

Since the second statement of modified Simmons mechanism is unrelated and insensitive, the degree of cooperation of the respondents with sensitive attributes is higher than that of modified Warner mechanism. On account of the respondent is only the requirement to report numbers in modified Christofides and the improved Christofides mechanisms. The degree of cooperation of the respondents with sensitive attributes is higher than that of modified Warner and Simmons mechanism. In the improved Christofides mechanism, none of the respondent knows the numbers others drew and the numbers others answered, which is proper in the real world. The freedom to know numbers others drew and numbers others answered is sacrificed in exchange for smaller variance under the same privacy budget ε .

We compare the variance and minimum sample size of modified Warner, Simmons, Christofides and the improved Christofides mechanisms using LDP as the common measurement of privacy leakage by theoretical analysis, numerical simulation and experiment based on a real world dataset. As a result, we find the improved Christofides mechanism for LDP framework. This is our third contribution.

7 CONCLUSION

In conclusion, we have modified Warner, Simmons and Christofides mechanism by drawing samples without replacement, thus reducing the variance of each mechanism. We then improve modified Christofides mechanism by sampling cards without replacement. Considering theoretical analysis, numerical simulation and experiment based on a real world dataset, we compared modified Warner, Simmons, Christofides and the improved Christofides mechanism using LDP as the measurement of privacy leakage. We found that the variance of modified Christofides mechanism was the smallest when the proportion of people with sensitive attributes $\pi_A < \pi_{A_1}$ or $\pi_A > \pi_{A_2}$, which is usually proper in the real world, and that the improved Christofides mechanism can be used to replace the Warner mechanism in sensitive issue investigation and LDP scenarios, as it offers a better trade-off between privacy budget, variance, and the degree of cooperation.

APPENDICES

A PROOF OF THEOREM 3.1

THEOREM 3.1 (MODIFIED CHRISTOFIDES MECHANISM VARIANCE). *The variance of $\hat{\pi}_A$ is*

$$\begin{aligned} \text{Var}\hat{\pi}_A &= \frac{\text{Var}\left(\sum_{i=1}^N X_i\right)}{N^2(L+1-2E(Y))^2} \\ &= \frac{\text{Var}Y}{N(L+1-2E(Y))^2}. \end{aligned}$$

PROOF. Firstly, we have

$$\begin{aligned} \text{Var}\left(\sum_{i=1}^N X_i\right) &= N\pi_A \left[\sum_{k=1}^L k^2 p_{L+1-k} - \left(\sum_{k=1}^L k p_{L+1-k} \right)^2 \right] + \\ &\quad N(1-\pi_A) \left[\sum_{k=1}^L k^2 p_k - \left(\sum_{k=1}^L k p_k \right)^2 \right] \\ &= N\pi_A \left[\sum_{k=1}^L (L+1-k)^2 p_k - \sum_{k=1}^L k^2 p_k \right] + \\ &\quad N\pi_A \left[-\left(\sum_{k=1}^L (L+1-k) p_k \right)^2 + \left(\sum_{k=1}^L k p_k \right)^2 \right] + \\ &\quad N \left[\sum_{k=1}^L k^2 p_k - \left(\sum_{k=1}^L k p_k \right)^2 \right] \\ &= N\pi_A \left[\sum_{k=1}^L ((L+1)^2 - 2(L+1)k) p_k \right] - \\ &\quad N\pi_A \left[-\left(\sum_{k=1}^L (L+1-k) p_k \right)^2 + \left(\sum_{k=1}^L k p_k \right)^2 \right] + \\ &\quad N\pi_A \left[\left(\sum_{k=1}^L ((L+1)p_k) \right) \left(\sum_{k=1}^L ((L+1-2k)p_k) \right) \right] \\ &= N \left[\sum_{k=1}^L k^2 p_k - \left(\sum_{k=1}^L k p_k \right)^2 \right]. \end{aligned}$$

Thus

$$\begin{aligned} \text{Var}\hat{\pi}_A &= \frac{\text{Var}\left(\frac{1}{N} \sum_{i=1}^N X_i\right)}{(L+1-2E(Y))^2} \\ &= \frac{\text{Var}Y}{N(L+1-2E(Y))^2}. \quad \square \end{aligned}$$

B PROOF OF THEOREM 4.1

THEOREM 4.1 (THE IMPROVED CHRISTOFIDES MECHANISM VARIANCE). *The variance of $\hat{\pi}_A$ is*

$$\begin{aligned} \text{Var}\hat{\pi}_A &= \frac{\text{Var}\left(\sum_{i=1}^N X_i\right)}{N^2(L+1-2E(Y))^2} \\ &= \frac{4\pi_A(1-\pi_A)\text{Var}(Y)}{(N-1)(L+1-2E(Y))^2}. \end{aligned}$$

PROOF. Since the estimator of π_A

$$\hat{\pi}_A = \frac{\frac{1}{N} \sum_{i=1}^N X_i - EY}{(L+1-2EY)},$$

with the variance

$$\begin{aligned} \text{Var}\hat{\pi}_A &= \text{Var}\left(\frac{\frac{1}{N} \sum_{i=1}^N X_i - EY}{L+1-2EY}\right) \\ &= \frac{1}{N^2(L+1-2EY)^2} \text{Var} \sum_{i=1}^N X_i \end{aligned}$$

,where

$$\begin{aligned}\text{Var} \sum_{i=1}^N X_i &= \mathbf{E} \left(\sum_{i=1}^N X_i \right)^2 - \left(\mathbf{E} \sum_{i=1}^N X_i \right)^2 \\ &= \sum_{i=1}^N \mathbf{E}(X_i^2) + \sum_{i \neq j} \mathbf{E}(X_i X_j) - \left(\mathbf{E} \sum_{i=1}^N X_i \right)^2.\end{aligned}$$

In the improved Christofides mechanism, X_i and X_j are no longer i.i.d. case, which yields difficulty in the proof. Here, both the participants and cards are sampled without replacement, which gives us dependent Y_i and Y_j , x_i and x_j , but Y_i and x_i are independent.

Firstly,

$$\begin{aligned}\sum_{i=1}^N \mathbf{E}(X_i^2) &= \sum_{i=1}^N \mathbf{E}[(L+1-Y_i)^2 x_i^2 + Y_i^2 x_i^2] \\ &= N [\mathbf{E}(L+1-Y)^2 \mathbf{E}x_i^2 + \mathbf{E}Y^2 \mathbf{E}(1-x_i)^2] \\ &= N [(L+1)^2 + \mathbf{E}Y^2 - 2(L+1)\mathbf{E}Y] \mathbf{E}x_i^2 + \\ &\quad N \mathbf{E}Y^2 \mathbf{E}(1-2x_i + x_i^2) \\ &= N \mathbf{E}Y^2 - 2N(L+1)\pi_A \mathbf{E}Y + N(L+1)^2 \pi_A.\end{aligned}\tag{6}$$

Secondly,

For $i \neq j$

$$\begin{aligned}\mathbf{E}X_i X_j &= \mathbf{E}((L+1-Y_i)x_i + Y_i(1-x_i)) \cdot \\ &\quad ((L+1-Y_j)x_j + Y_j(1-x_j)), \\ &= \mathbf{E}(L+1-Y_i)(L+1-Y_j) \mathbf{E}x_i x_j \\ &\quad + \mathbf{E}Y_i Y_j \mathbf{E}(1-x_i)(1-x_j) \\ &\quad + 2\mathbf{E}Y_i(L+1-Y_j) \mathbf{E}(1-x_i)x_j.\end{aligned}$$

Because we have

$$\begin{aligned}\mathbf{E}Y_i Y_j &= \sum_{m=1}^N \sum_{n=1}^N mn \mathbf{P}(Y_i = m, Y_j = n) \\ &= \sum_{m=1}^N m \left(\sum_{k \neq m}^N n p_m \frac{p_n N}{N-1} + m p_m \frac{p_m N-1}{N-1} \right) \\ &= \frac{N}{N-1} \mathbf{E}Y \sum_{m=1}^N m p_m - \frac{1}{N-1} \sum_{m=1}^N m^2 p_l \\ &= (\mathbf{E}Y)^2 - \frac{1}{N-1} \text{Var}Y.\end{aligned}$$

and

$$\mathbf{E}x_i = \mathbf{P}(x_i = 1) = \pi_A$$

$$\mathbf{E}x_i x_j = \mathbf{P}(x_i = 1, x_j = 1) = \frac{C_{N\pi_A}^2}{C_N^2}$$

$$\mathbf{E}(1-x_i)(1-x_j)(i \neq j) = \mathbf{P}(x_i = 0, x_j = 0) = \frac{C_{N-N\pi_A}^2}{C_N^2}$$

$$\mathbf{E}(1-x_i)x_j(i \neq j) = \mathbf{P}(x_i = 0, x_j = 1) = \frac{C_{N\pi_A}^1 C_{N-N\pi_A}^1}{A_N^2}.$$

We can get

$$\begin{aligned}\mathbf{E}X_i X_j &= \mathbf{E}[(L+1)^2 - Y_i(L+1) + Y_i Y_j] \mathbf{E}x_i x_j + \mathbf{E}Y_i Y_j \\ &\quad \mathbf{E}(1-x_i)(1-x_j) + \mathbf{E}(L+1-Y_i)Y_j \mathbf{E}x_i(1-x_j) + \\ &\quad \mathbf{E}Y_i(L+1-Y_j) \mathbf{E}(1-x_i)x_j \\ &= \mathbf{E}Y_i Y_j [\mathbf{E}x_i x_j + \mathbf{E}(1-x_i)(1-x_j) - \mathbf{E}x_i(1-x_j) - \\ &\quad \mathbf{E}(1-x_i)x_j] + \mathbf{E}Y[-2(L+1)\mathbf{E}x_i x_j + (L+1)\mathbf{E}x_i \\ &\quad (1-x_j) + (L+1)\mathbf{E}(1-x_i)x_j] + (L+1)^2 \mathbf{E}x_i x_j \\ &= [N\pi_A(N\pi_A-1) + (N-N\pi_A)(N-N\pi_A-1) - \\ &\quad 2N + \pi_A(N-N\pi_A)] \mathbf{E}Y_i Y_j + [-2(L+1)N\pi_A(N\pi_A- \\ &\quad 1) + 2(L+1)N\pi_A(N-N\pi_A)] \mathbf{E}Y + (L+1)^2 N\pi_A \\ &\quad (N\pi_A-1) \\ &= [4N^2\pi_A^2 - 4N^2\pi_A + N^2 - N] \mathbf{E}Y_i Y_j + 2(L+1) \\ &\quad N\pi_A[1+N-2N\pi_A] \mathbf{E}Y + (L+1)^2 N\pi_A(N\pi_A-1) \\ &= [4N^2\pi_A^2 - 4N^2\pi_A + N^2 - N] [(\mathbf{E}Y)^2 - \frac{1}{N-1} \\ &\quad \text{Var}Y] + 2(L+1)N\pi_A[1+N-2N\pi_A] \mathbf{E}Y + (L+1)^2 \\ &\quad N\pi_A(N\pi_A-1).\end{aligned}\tag{7}$$

Thirdly,

$$\begin{aligned}\mathbf{E}(\sum_{i=1}^N X_i)^2 &= N^2 [\mathbf{E}Y + \pi_A(L+1-2\mathbf{E}Y)]^2 \\ &= N^2 [(L+1)\pi_A + (1-2\pi_A)\mathbf{E}Y]^2 \\ &= N^2 [(L+1)^2 \pi_A^2 + (1-2\pi_A)^2 (\mathbf{E}Y)^2 + 2(L+1)\pi_A \\ &\quad (1-2\pi_A)\mathbf{E}Y].\end{aligned}\tag{8}$$

Finally, combine equation(6), (7) and (8), the variance of the estimator $\hat{\pi}_A$ is

$$\begin{aligned}\text{Var}\hat{\pi}_A &= \frac{1}{N^2(L+1-2\mathbf{E}Y)^2} \text{Var} \sum_{i=1}^N X_i \\ &= \frac{4\pi_A(1-\pi_A)\text{Var}Y}{(N-1)(L+1-2\mathbf{E}Y)^2}. \quad \square\end{aligned}$$

C PROOF OF THEOREM 5.3

THEOREM 5.3 (MODIFIED SIMMONS MECHANISM VARIANCE VERSUS EPSILON). When $\pi_B = 1/2$, the variance Var_{π_A} obtains minimum as following

$$\text{Var}\hat{\pi}_A = \frac{e^\epsilon}{N(e^\epsilon - 1)^2}.$$

PROOF. Substitute (4) into (2). The variance can be written as

$$(1) \text{ When } \pi_B \leq \frac{1}{2},$$

$$\begin{aligned}\text{Var}\hat{\pi}_A &= \frac{\left(\frac{1}{e^\epsilon-1} + \pi_A\right) \left(1 + \frac{1}{(e^\epsilon-1)\pi_B}\right)}{N} - \frac{1}{N(e^\epsilon-1)^2} \\ &\quad - \frac{(e^\epsilon+1)\pi_A}{N(e^\epsilon-1)}\end{aligned}$$

$$\min \text{Var}\hat{\pi}_A = \text{Var}\hat{\pi}_A|_{\pi_B=\frac{1}{2}} = \frac{e^\epsilon}{N(e^\epsilon-1)^2}.$$

(2) When $\pi_B > \frac{1}{2}$,

$$\begin{aligned} \text{Var}\hat{\pi}_A &= \frac{\left(\frac{1}{e^\varepsilon - 1} + \pi_A\right) \left(1 + \frac{1}{(e^\varepsilon - 1)(1 - \pi_B)}\right)}{N} - \frac{1}{N(e^\varepsilon - 1)^2} \\ &\quad - \frac{(e^\varepsilon + 1)\pi_A}{N(e^\varepsilon - 1)} \\ \min \text{Var}\hat{\pi}_A &= \text{Var}\hat{\pi}_A|_{\pi_B = \frac{1}{2}} = \frac{e^\varepsilon}{N(e^\varepsilon - 1)^2}. \end{aligned}$$

So the variance of the estimator $\hat{\pi}_A$ is

$$\text{Var}\hat{\pi}_A = \frac{e^\varepsilon}{N(e^\varepsilon - 1)^2}. \quad \square$$

D PROOF OF THEOREM 5.5

THEOREM 5.5 (MODIFIED CHRISTOFIDES MECHANISM VARIANCE VERSUS EPSILON). *For the case $L = 3$, the variance of the modified Christofides mechanism Var_{MC} arrives its minimum*

$$\text{Var}\hat{\pi}_A = \frac{1}{4N} \left[\frac{(e^\varepsilon + 1)^2}{(e^\varepsilon - 1)^2(1 - p_2)} - 1 \right]$$

under the situation that proportions

$$p_1 = (1 - p_2) / (e^\varepsilon + 1), p_3 = [e^\varepsilon(1 - p_2)] / (e^\varepsilon + 1)$$

or

$$p_1 = [e^\varepsilon(1 - p_2)] / (e^\varepsilon + 1), p_3 = (1 - p_2) / (e^\varepsilon + 1).$$

PROOF. The expectation of Y is

$$\begin{aligned} \text{E}Y &= p_1 + p_2 + 3(1 - p_1 - p_2) \\ &= 3 - 2p_1 - p_2. \end{aligned}$$

The variance of Y is

$$\begin{aligned} \text{Var}Y &= p_1 + 4p_2 + 9(1 - p_1 - p_2) - (3 - 2p_1 - p_2)^2 \\ &= 4p_1 + p_2 - 4p_1^2 - p_2^2 - 4p_1p_2. \end{aligned}$$

$$\begin{aligned} \text{Var}\hat{\pi}_A &= \frac{\text{Var}Y}{N(3 + 1 - 2\text{E}Y)^2} \\ &= \frac{4p_1 + p_2 - 4p_1^2 - p_2^2 - 4p_1p_2}{N[3 + 1 - 2(3 - 2p_1 - p_2)]^2} \\ &= \frac{4p_1 + p_2 - 4p_1^2 - p_2^2 - 4p_1p_2}{N(4p_1 + 2p_2 - 2)^2} \\ &= f(p_1, p_2). \end{aligned}$$

Now let's minimize the function $f(p_1, p_2)$. Since

$$\begin{aligned} \frac{\partial f(p_1, p_2)}{\partial p_2} &= \frac{(1 - 4p_1 - 2p_2)(4p_1 + 2p_2 - 2)^2}{N(4p_1 + 2p_2 - 2)^4} - \\ &\quad \frac{4(4p_1 + p_2 - 4p_1^2 - p_2^2 - 4p_1p_2)(4p_1 + 2p_2 - 2)}{N(4p_1 + 2p_2 - 2)^4} \\ &= \frac{\left(p_1 + \frac{1 - p_2}{2}\right) \left(p_1 - \frac{1 - p_2}{2}\right)}{N(2p_1 + p_2 - 1)^4} \\ &\neq 0. \end{aligned}$$

the function $f(p_1, p_2)$ has no extremum. The maximum or minimum points must be boundary points.

Since

$$\frac{1}{e^\varepsilon} p_1 \leq p_3 = 1 - p_1 - p_2 \leq e^\varepsilon p_1$$

thus

$$\frac{1 - p_2}{e^\varepsilon + 1} \leq p_1 \leq \frac{e^\varepsilon}{e^\varepsilon + 1} (1 - p_2).$$

Because the function for the two bounding points

$$\begin{aligned} f(p_1, p_2)|_{p_1 = \frac{1 - p_2}{e^\varepsilon + 1}} &= \frac{4\frac{1 - p_2}{e^\varepsilon + 1} + p_2 - 4\left(\frac{1 - p_2}{e^\varepsilon + 1}\right)^2 - p_2^2 - 4\frac{1 - p_2}{e^\varepsilon + 1}p_2}{N\left[4\frac{1 - p_2}{e^\varepsilon + 1} + 2p_2 - 2\right]^2} \\ &= \frac{1}{4N} \left[\frac{(e^\varepsilon + 1)^2}{(e^\varepsilon - 1)^2(1 - p_2)} - 1 \right] \end{aligned}$$

$$\begin{aligned} f(p_1, p_2)|_{p_1 = \frac{e^\varepsilon(1 - p_2)}{e^\varepsilon + 1}} &= \frac{4\frac{e^\varepsilon(1 - p_2)}{e^\varepsilon + 1} + p_2 - 4\left(\frac{e^\varepsilon(1 - p_2)}{e^\varepsilon + 1}\right)^2}{N\left[\frac{e^\varepsilon}{e^\varepsilon + 1}(1 - p_2) + 2p_2 - 2\right]^2} - \\ &\quad \frac{p_2^2 + 4\frac{e^\varepsilon}{e^\varepsilon + 1}(1 - p_2)p_2}{N\left[\frac{e^\varepsilon}{e^\varepsilon + 1}(1 - p_2) + 2p_2 - 2\right]^2} \\ &= \frac{1}{4N} \left[\frac{(e^\varepsilon + 1)^2}{(e^\varepsilon - 1)^2(1 - p_2)} - 1 \right] \end{aligned}$$

and

$$f(p_1, p_2)|_{p_1 = \frac{1 - p_2}{2}} \rightarrow \infty.$$

Therefore

$$\min f(p_1, p_2) = f\left(\frac{1 - p_2}{e^\varepsilon + 1}, p_2\right) = f\left(\frac{e^\varepsilon(1 - p_2)}{e^\varepsilon + 1}, p_2\right).$$

So

$$\text{Var}\hat{\pi}_A = \frac{1}{4N} \left[\frac{(e^\varepsilon + 1)^2}{(e^\varepsilon - 1)^2(1 - p_2)} - 1 \right]. \quad \square$$

ACKNOWLEDGMENTS

This research has been supported by National Key R&D Program of China (2022YFB4501500, 2022YFB4501504) and Zhejiang Lab (2022NF0AC01). Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not reflect the views of the funding agencies.

REFERENCES

- [1] Rafal Ablamowicz and Bertfried Fauser. 2023. *Harvard's secure data classifications*. Harvard University Privacy Tools Project. Retrieved February 15, 2023 from <http://psiprivacy.org/>
- [2] Shunsuke Aoki, Masayuki Iwai, and Kaoru Sezaki. 2012. Limited negative surveys: Privacy-preserving participatory sensing. In *2012 IEEE 1st International Conference on Cloud Networking (CLOUDNET)*. IEEE, 158–160.
- [3] Hilal Asi, Vitaly Feldman, and Kunal Talwar. 2022. Optimal algorithms for mean estimation under local differential privacy. In *International Conference on Machine Learning*. PMLR, 1046–1056.
- [4] Ergute Bao, Yin Yang, Xiaokui Xiao, and Bolin Ding. 2021. CGM: an enhanced mechanism for streaming data collection with local differential privacy. *Proceedings of the VLDB Endowment* 14, 11 (2021), 2258–2270.
- [5] Raef Bassily, Kobbi Nissim, Uri Stemmer, and Abhradeep Guha Thakurta. 2017. Practical locally private heavy hitters. *Advances in Neural Information Processing Systems* 30 (2017).
- [6] United States Census Bureau. 2020. *United States Census Bureau*. the United States government. Retrieved February 23, 2023 from <https://onhemap.ces.census.gov/>
- [7] Yang Cao, Masatoshi Yoshikawa, Yonghui Xiao, and Li Xiong. 2018. Quantifying differential privacy in continuous data release under temporal correlations. *IEEE transactions on knowledge and data engineering* 31, 7 (2018), 1281–1295.
- [8] Tasos C Christofides. 2003. A generalized randomized response technique. *Metrika* 57 (2003), 195–200.
- [9] Graham Cormode, Samuel Maddock, and Carsten Maple. 2021. Frequency estimation under local differential privacy. *Proceedings of the VLDB Endowment* 14, 11 (2021), 2046–2058.
- [10] Bolin Ding, Janardhan Kulkarni, and Sergey Yekhanin. 2017. Collecting telemetry data privately. *Advances in Neural Information Processing Systems* 30 (2017).
- [11] John C Duchi, Michael I Jordan, and Martin J Wainwright. 2013. Local privacy and statistical minimax rates. In *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*. IEEE, 429–438.
- [12] Rick Durrett. 2019. *Probability: theory and examples*. Vol. 49. Cambridge university press.
- [13] Úlfar Erlingsson, Vasyl Pihur, and Aleksandra Korolova. 2014. Rappor: Randomized aggregatable privacy-preserving ordinal response. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*. 1054–1067.
- [14] Fernando Esponda. 2006. Negative surveys. *arXiv preprint math/0608176* (2006).
- [15] Sabrina Giordano and Pier Francesco Perri. 2012. Efficiency comparison of unrelated question models based on same privacy protection degree. *Statistical Papers* 53, 4 (2012), 987.
- [16] Christopher R Gjestvang and Sarjinder Singh. 2006. A new randomized response model. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)* 68, 3 (2006), 523–530.
- [17] Bernard G Greenberg, Abdel-Latif A Abul-Ela, Walt R Simmons, and Daniel G Horvitz. 1969. The unrelated question randomized response model: Theoretical framework. *J. Amer. Statist. Assoc.* 64, 326 (1969), 520–539.
- [18] Anthony YC Kuk. 1990. Asking sensitive questions indirectly. *Biometrika* 77, 2 (1990), 436–438.
- [19] Jan Lanke. 1976. On the degree of protection in randomized interviews. *International Statistical Review/Revue Internationale de Statistique* (1976), 197–203.
- [20] Frederick W Leysieffer and Stanley L Warner. 1976. Respondent jeopardy and optimal designs in randomized response models. *J. Amer. Statist. Assoc.* 71, 355 (1976), 649–656.
- [21] NS Mangat and Ravindra Singh. 1990. An alternative randomized response procedure. *Biometrika* 77, 2 (1990), 439–442.
- [22] Naurang S Mangat. 1994. An improved randomized response strategy. *Journal of the Royal Statistical Society: Series B (Methodological)* 56, 1 (1994), 93–95.
- [23] Pier Francesco Perri. 2008. Modified randomized devices for Simmons' model. *Model Assisted Statistics and Applications* 3, 3 (2008), 233–239.
- [24] Sofya Raskhodnikova, Adam Smith, Homin K Lee, Kobbi Nissim, and Shiva Prasad Kasiviswanathan. 2008. What can we learn privately. In *Proceedings of the 54th Annual Symposium on Foundations of Computer Science*. 531–540.
- [25] Sarjinder Singh, Stephen Horn, Ravindra Singh, and NS Mangat. 2003. On the use of modified randomization device for estimating the prevalence of a sensitive attribute. *Statistics in transition* 6, 4 (2003), 515–522.
- [26] Apple Differential Privacy Team. 2017. *Learning with privacy at scale*. Apple. Retrieved March 1, 2023 from <https://machinelearning.apple.com/research/learning-with-privacy-at-scale>
- [27] Integrated Public Use Microdata Series (IPUMS USA). 2021. *Description of HCO-VAN2021 dataset*. Integrated Public Use Microdata Series (IPUMS USA). Retrieved February 15, 2023 from https://usa.ipums.org/usa/acs_healthins.shtml
- [28] Tianhao Wang and Jeremiah Blocki. 2017. Locally differentially private protocols for frequency estimation. In *Proceedings of the 26th USENIX Security Symposium*.
- [29] Tianhao Wang, Ninghui Li, and Somesh Jha. 2018. Locally differentially private frequent itemset mining. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 127–143.
- [30] Tianhao Wang, Milan Lopuhaa-Zwakenberg, Zitao Li, Boris Skoric, and Ninghui Li. 2020. Locally Differentially Private Frequency Estimation with Consistency. In *NDSS'20: Proceedings of the NDSS Symposium*.
- [31] Stanley L Warner. 1965. Randomized response: A survey technique for eliminating evasive answer bias. *J. Amer. Statist. Assoc.* 60, 309 (1965), 63–69.
- [32] Atsushi Waseda and Ryo Nojima. 2016. Analyzing randomized response mechanisms under differential privacy. In *Information Security: 19th International Conference, ISC 2016, Honolulu, HI, USA, September 3–6, 2016. Proceedings* 19. Springer, 271–282.
- [33] Zhuolun Xiang, Bolin Ding, Xi He, and Jingren Zhou. 2020. Linear and range counting under metric-based local differential privacy. In *2020 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 908–913.
- [34] Jianyu Yang, Tianhao Wang, Ninghui Li, Xiang Cheng, and Sen Su. 2020. Answering multi-dimensional range queries under local differential privacy. *Proceedings of the VLDB Endowment* 14, 3 (2020), 378–390.