Asymmetric Differential Privacy

Shun Takagi
Kyoto University
Japan
takagi.shun.45a@st.kyoto-u.ac.jp

Fumiyuki Kato
Kyoto University
Japan
kato.fumiyuki.68z@st.kyoto-u.ac.jp

Yang Cao
Hokkaido University
Japan
yang@ist.hokudai.ac.jp

Masatoshi Yoshikawa
Kyoto University
Japan
yoshikawa@i.kyoto-u.ac.jp

Abstract—Differential privacy (DP) is attracting considerable research attention as a privacy definition when publishing statistics of a dataset. This study focused on addressing the limitation that DP inevitably causes two-sided errors. For example, consider a threshold query that asks whether a count is above a given threshold or not. An answer through the DP mechanism can cause error. This phenomenon is not desirable for sensitive analysis such as the counting of COVID-19-infected individuals (in a dataset) visiting a specific location; misinformation can result in incorrect decision-making which can increase the epidemic. To the best of our knowledge, the problem is yet to be solved. We proposed a variation of DP, namely asymmetric DP (ADP) to solve the problem. ADP can provide reasonable privacy protection and achieve one-sided errors. Finally, experiments were conducted to evaluate the utility of the proposed mechanism for the epidemic analysis using a real-world dataset. The results of study revealed the feasibility of proposed mechanisms.

Index Terms—Differential Privacy, One-sided Error, Location Privacy

I. INTRODUCTION

Differential privacy (DP) [1] is becoming the standard in privacy notion. The US Census adopted DP when publishing the 2020 Census results [2], and IT companies, such as Google [3], Apple [4], Microsoft [5], and Uber [6], are using DP to protect privacy while collecting data. This widespread adoption originates from mathematical rigorfulness under the assumption that an adversary has any knowledge about an individual’s data in a dataset.

However, the rigor of DP results in utility limitations. We focused on a utility limitation, namely two-sided error, which occurs when solving a decision problem (i.e., a query whose answer is binary \{True, False\}) by a randomized algorithm such as a Monte Carlo algorithm [7]. To the best of our knowledge, this study is the first to consider this type of error in DP. Two sided is the characteristic that both potential answers True and False may be wrong. Thus, an algorithm causes false positives and false negatives. By contrast, one sided denotes the characteristic that either false positive or false negative occurs. Without the loss of generality, error is one sided if only a false negative occurs. Thus, if the error is one sided, a guarantee of accuracy exists for an answer marked as True.

For an example of two-sided errors, statistics of trajectories of infected people are published to control epidemic diseases such as COVID-19 [8] as displayed in Figure 1. We queried whether a location is safe or not with respect to epidemic disease by a threshold query (i.e., a decision problem that queries whether a count is under the threshold or not). Although DP can be used to answer the query with privacy protection, answering a decision problem by any DP mechanism always causes two-sided error. Thus, even if published information says safe (dangerous) for a target location, the location may not be safe (not be dangerous) because of noise. This published information may spread the epidemic rather than containing it. Therefore, published information with two-sided errors may not be appropriate for high-risk scenarios such as epidemic analysis.

Specifically, in Figure 1, we query “is location c under the threshold?”. The true answer is True, but any ε-DP mechanism outputs False with some probability (the existence of false negative). Similarly, for the query “is location b under the threshold?”, the true answer is False, but any ε-DP mechanism outputs True with some probability (the existence of a false positive). Therefore, the error is a two-sided error. In this example, the false positive involves a high risk with respect to the epidemic disease, but the false negative does not. Therefore, we achieved one-sided errors with formal privacy.
We proposed asymmetric differential privacy (ADP), which is derived from a necessary condition to achieve one-sided errors. ADP definition considers a new neighboring relationship, which may seem trivial; however, no existing privacy definition expresses the reasonable privacy protection for the problem of Figure 1. Therefore, we introduce ADP.

We proposed mechanisms following ADP. First, a primitive mechanism which is the ADP version of the Laplace mechanism [9], called the asymmetric Laplace mechanism (ALap), was proposed. We showed that ALap achieved one-sided errors.

Finally, we conducted the experiments using the real-world dataset. The experiment revealed that the proposed mechanism is sufficiently feasible for location monitoring with one-sided errors. We show the example of a result in Figure 2. These represent the safe, dangerous, and obscure states at locations on the Tokyo map at 6 p.m. published by mechanisms following no privacy (ground truth), ε-DP, (ε, δ)-DP, and (ε, p)-ADP under the assumption that “a trajectory does not include the target location” is nonsensitive, which is described by p. A safe spot, a dangerous spot, and an obscure spot represent a location visited at 6 p.m. by less than 3, equal to or larger than 3, and the unclear number of infected people due to the noise, respectively. Here, ε-DP and (ε, δ) denotes obscure for almost all spots, ADP can publish many accurate safe spots.

The contributions of the study are as follows:

- ADP was proposed to solve the issues. We show that ADP provides reasonable privacy protection for publishing safe information with one-sided errors under the assumption that information “one did not visit a target location” is nonsensitive.
- We proposed a novel mechanism, ALap.
- Our experiments using the real-world dataset revealed the feasibility of the mechanism for location monitoring.

A. Related Work

The most popular relaxation of DP is (ε, δ)-DP [10], and δ represents the probability that a mechanism breaks ε-DP. Experts warn that (ε, δ)-DP allows an unacceptable mechanism. Therefore, (ε, δ)-DP is not suitable for the proposed problem.

Another method to relax DP is the same as ours: redefining the definition of a neighboring relationship. Blowfish privacy [11] and one-sided differential privacy (OSDP) [12] belong to this family. However, we also show that their privacy definitions cause unreasonable privacy leaks to achieve one-sided errors for the problem in Figure 1.

OSDP: In OSDP, nonsensitive records are used to improve utility [12]. The motivation of this method differs from ours, but OSDP implicitly catches asymmetric neighboring relationship (i.e., X is neighboring to X′, but X′ is not neighboring to X). Therefore, OSDP may solve the limitation of two-sided errors in specific cases, but the privacy of OSDP is not sufficiently expressive to tightly relax the privacy protection of DP for one-sided errors. OSDP only determines whether certain records are protected or not, and OSDP cannot specify which property of a record is protected. Therefore, OSDP is not sufficiently flexible to stipulate reasonable privacy protection for one-sided errors.

Blowfish privacy: Blowfish privacy (and Pufffish privacy) also redefines the neighboring relationship [11], [13]. Blowfish privacy can specify the property of a record that is protected, but the definition cannot express the asymmetric neighboring relationship. Therefore, blowfish privacy is also not sufficiently flexible, which results in unexpected privacy leaks.

II. BACKGROUND

We first introduced DP and related definitions, which are the bases of our proposed notions. Second, we explain counting query, decision problem, and one-sided error this study handles. Finally, we show the problem setting of this paper.

The notations used in this paper are listed in Table I.

A. DP

DP [1] is a mathematical privacy definition that quantitatively evaluates the privacy protection of a randomized mechanism. A randomized mechanism M is a randomized function that takes a dataset as input and randomly returns z ∈ Z. For preliminary, we introduce the definition of the neighboring relationship of DP.

Definition II.1 (Neighboring relationship). X is neighboring to X′ with respect to x and x′ if X′ is constructed by replacing
one record that is \(x\) of \(X\) with \(x'\). This relationship is denoted by \(X \sim_{x,x'} X'\) or simply \(X \sim X'\).

Next, we introduce the definition of approximate DP denoted by \((\varepsilon, \delta)\)-DP, which is the most popular generalization of DP.

**Definition II.2** \((\varepsilon, \delta)\)-DP. A randomized mechanism \(M\) satisfies \((\varepsilon, \delta)\)-DP iff \(\forall X, X' \in \mathcal{X}^n\) such that \(X \sim X'\) and \(\forall S \subseteq \mathcal{Z}\),

\[
\Pr[M(X) \in S] \leq e^\varepsilon \Pr[M(X') \in S] + \delta,
\]

where \(\mathcal{X}^n\) and \(\mathcal{Z}\) are the universe of a dataset and an output, respectively. Simply \(\varepsilon\)-DP denotes \((\varepsilon, 0)\)-DP.

**B. Problem Setting: Decision Problem**

In this study, as a decision problem\(^2\), we introduce a threshold proposition to the answer of a counting query. Here, we describe the definitions of counting query, threshold proposition, and one-sided errors. Next, we describe the problem setting of this study using these notions.

1) **Counting Query:** Counting query is one of the most basic statistical queries. Counting query appears in the fractional form, with weights (linear query), or in more complex form. However, in this study, the most simple type of counting query \(f_C : \mathcal{X}^n \rightarrow \{0, 1, \ldots, n\}\), which counts the numbers of records satisfying each condition \(c_1, \ldots, c_d\), where \(C = (c_1, \ldots, c_d)\) is a tuple of propositional functions to a record, is considered.

2) **Threshold proposition:** The threshold proposition is a simple proposition to determine whether the number is above (under) the threshold or not.

**Definition II.3.** Threshold proposition \(p_{\leq t}^\varepsilon : \mathbb{N} \rightarrow \{\text{False}, \text{True}\}\) is the propositional function such that

\[
p_{\leq t}^\varepsilon(m) = \begin{cases} 
\text{True} & \text{if } m \leq t \\
\text{False} & \text{otherwise}
\end{cases}
\]

We define \(p_{\geq t}^\varepsilon(m)\) to determine whether \(m\) is above \(t\) or not.

\(^2\)We assume a data-dependent decision problem \(q\) (i.e., \(\exists X, X' \in \mathcal{X}^n, q(X) \neq q(X')\)).

3) \((q, \alpha, \beta)\)-one-sided error: One-sided error is first defined on the Monte Carlo algorithm [14] that is randomized to answer problems that are difficult with respect to complexity. An algorithm is one sided if the output True is always correct (i.e., true-biased). Then, one-sided error is defined on the one-sided algorithm as the probability that the algorithm wrongly outputs False.

To comprehensively investigate the DP characteristic with respect to one-sided errors, we generalize one-sided errors. Intuitively, we allow errors occurring with small probability \(\alpha\) for the answer True. In this state, if the probability that a mechanism wrongly outputs False is lower than \(1 - \beta\), then the mechanism is \((q, \alpha, \beta)\)-one-sided. Formally,

**Definition II.4** \((q, \alpha, \beta)\)-one-sided. Mechanism \(M\) is \((q, \alpha, \beta)\)-one-sided for \(X\) such that \(q(X) = \text{True}\) if \(\forall X' \in \mathcal{X}^n\) such that \(q(X') = \text{False}\), there exists \(p_{\text{san}} : \mathcal{Z} \rightarrow \{\text{False}, \text{True}\}\) such that \(\Pr[p_{\text{san}} \circ M(X') = \text{True}] < \alpha\) and \(\Pr[p_{\text{san}} \circ M(X) = \text{True}] \geq \beta\).

Here, \(p_{\text{san}}\) works like a sanitizer [15] to answer \(q\). We call such \(p_{\text{san}}(q, \alpha, \beta)\)-sanitizer. We can obtain \(q(X) = \text{True}\) with high probability (i.e., \(1 - \alpha\)) when we see output True from a \((q, \alpha, \beta)\)-sanitizer. For example, if \(M\) is \((q, 0, \beta)\)-one-sided for \(X\), a post-processing function \(p_{\text{san}}\) exist such that the answer True of \(p_{\text{san}} \circ M(X)\) is always true and the one-sided error is lower than \(1 - \beta\).

4) **Problem Setting:** Formally, a mechanism that is one sided is considered to answer the following queries in a manner that preserves privacy. Given target locations \((l_1, l_2, \ldots, l_d)\) and time \(T\) for \(i \in [d]\), about an epidemic disease,

\[
q_{\leq}^i = p_{\leq}^t \circ f_C(\cdot); \text{ location } l_i \text{ is not an epicenter?}
\]

\[
q_{\geq}^i = p_{\geq}^t \circ f_C(\cdot); \text{ location } l_i \text{ is an epicenter?}
\]

where \(f_C = (c_1^i, c_2^i, \ldots, c_d^i)\) and \(c_j^i(x)\) determines whether trajectory \(x\) includes location \(l_i\) in time \(T\) or not.

**III. ASYMMETRIC DP**

As in the previous section, existing privacy definitions result in unreasonable privacy protection to achieve one-sided errors. To solve this problem, we proposed ADP to provide reasonable privacy protection while achieving one-sided errors.

First, we define ADP. Second, we state the privacy guarantee (\(p\)-neighboring relationship). Third, we introduce \(p_{\leq}\) and \(p_{\geq}\), which are policies to answer \(q_{\leq}\) and \(q_{\geq}\) (see Section II-B4 for them) with one-sided errors.

**A. Definition**

First, we define a new neighboring relationship, called \(p\)-neighboring relationship, using propositional function \(p : X \rightarrow \{\text{False}, \text{True}\}\) called policy. Formally,

**Definition III.1** \((p\)-neighboring relationship). Given two datasets \(X\) and \(X'\), \(X\) is \(p\)-neighboring to \(X'\), if \(X \sim_{x,x'} X'\) and \((-p(x) \lor (p(x) \land p(x'))) = \text{False}\) (i.e., \((p(x) \rightarrow p(x')) = \text{False}\)). We denote this relationship by \(X \sim_{x,x'} X'\) (or simply \(X \sim_{p} X'\)).
Here, $X \sim^p X'$ does not mean $X' \sim^p X$, which is the origin of the name of asymmetric DP. Based on $p$-neighboring relationship, we define ADP.

**Definition III.2** (ADP). Randomized mechanism $M$ satisfies $(\varepsilon, p)$-ADP iff $\forall x \in X, X, X'$ such that $X \sim^p X'$,
\[
\Pr[M(X) = z] \leq e^\varepsilon \Pr[M(X') = z].
\]

**B. Policies**

We introduced policies to achieve one-sided errors for $q_{\leq}^i$ and $q_{\geq}^i$, respectively. Setting $-c_t^i$ and $c_t^i$ allows one-sided errors for $q_{\leq}^i$ and $q_{\geq}^i$, respectively.

1) **Policy for $q_{\leq}^i$**: We introduce $p$ such that $\forall x \in X$, $c_t^i(x) \rightarrow p(x) = \text{True}$. Next, using such $p$, we analyze one-sided errors of an $(\varepsilon, p)$-ADP mechanism. We first introduced the minimum path instead of the hamming distance in DP.

**Definition III.3** (the minimum path). The minimum path from $X$ to $X'$, denoted by $d_{\text{min}}^p(X, X')$, is the minimum number of steps to change $X$ to $X'$ using $p$-neighboring datasets.

If $d_{\text{min}}^p(X, X') = k$, a $k$ steps path exists. Using the minimum path, the one-sided error of an $(\varepsilon, p)$-ADP mechanism can be analyzed as follows:

**Proposition III.4.** If $(\varepsilon, p)$-ADP mechanism is $(q, \alpha, \beta)$-one-sided for $X$, $\varepsilon \geq \frac{\log((1-\alpha)/(1-\beta))}{k(X)}$, where $k(X) = \min\{x' | q(X') = \text{False}\}\{d_{\text{min}}^p(X, X')\}$.

Here, $\varepsilon$ can be a small value even when $\alpha = 0$ by relaxation of $p$. This relaxation of $p$ leads to the leakage of the information that the user did not visit the location $l_i$. The information is nonsensitive. Therefore, we adopt this policy.

2) **Policy for $q_{\geq}^i$**: For a mechanism to be $(q_{\geq}^i, \alpha, \beta)$-one-sided and achieve $(\varepsilon, p)$-ADP, we introduced $p$ such that $\forall x \in X$, $c_t^i(x) \rightarrow p(x) = \text{True}$. However, such a policy is not feasible from the privacy perspective. Therefore, we did not adopt this policy. Therefore, the proposed mechanism provides the same performance for $q_{\geq}^i$ as $\varepsilon$-DP.

**IV. MECHANISM**

We proposed a mechanism that is $(q_{\leq}^i, \alpha, \beta)$-one-sided and satisfies $(\varepsilon, p)$-ADP.

**A. Asymmetric Laplace mechanism**

An asymmetric Laplace mechanism (ALap), the ADP version of the Laplace mechanism, was introduced as the most basic mechanism. ALap perturbs the answer of counting query $f : X^n \rightarrow \mathbb{R}^d$. First, we define $p$-sensitivity, which corresponds to the notion of sensitivity of DP. Next, we define ALap using $p$-sensitivity.

1) **$p$-sensitivity**: We define $p$-sensitivity of query $f : X^n \rightarrow \mathbb{R}^d$ as the sensitivity induced by policy $p$.

**Definition IV.1** ($p$-sensitivity of $f$). Given $p : X \rightarrow \{\text{True}, \text{False}\}$, we define $p$-sensitivity of $f$, denoted by $\Delta_p$, as follows: $\Delta_p(f) := \sup_{X \sim^p X'} ||f(X') - f(X)||_1$.

$p$-sensitivity exhibits a unique characteristic called monotonicity, which does not appear in DP sensitivity.

**Definition IV.2** (Monotonicity of $p$-sensitivity). The $p$-sensitivity of $f(\cdot)$, $(\Delta_p(f(\cdot)))$ is monotonically increasing (decreasing) if $\forall x \sim^p x'$, $f(x)_i \leq f(x')_i$ $(f(x)_i \geq f(x')_i)$. If for all $i \in [d]$, $\Delta_p(f(\cdot)_i)$ is monotonically increasing (decreasing), then the $p$-sensitivity of $f$ is monotonically increasing (decreasing). We define function $\text{Sign}_p$, which discriminates monotonicity. $\text{Sign}_p(f(\cdot)_i) := \begin{cases} +1 & \text{if } \Delta_p(f(\cdot)_i) \text{ is monotonically increasing} \\ -1 & \text{if } \Delta_p(f(\cdot)_i) \text{ is monotonically decreasing} \end{cases}$

2) **Definition**: We proposed ALap, which is related to the answer of query $f : X^n \rightarrow \mathbb{R}^d$ according to $p$-sensitivity.

**Definition IV.3** (Asymmetric Laplace mechanism). Given query $f : X^n \rightarrow \mathbb{R}^d$, policy $p$, and privacy parameter $\varepsilon$, the asymmetric Laplace mechanism ALap is as follows: ALap$_{p, \varepsilon, f}(X) = f(X) + (\lambda_1, \ldots, \lambda_d)$, where $\lambda_i$ is independently distributed and follows the distribution for each $i \in [d]$.

If $p$-sensitivity of $f(\cdot)_i$ is monotonic,
\[
\begin{cases} \frac{\varepsilon}{\Delta_p(f(\cdot)_i)} \exp^{-\text{Sign}_p(f(\cdot)_i)\varepsilon} \lambda_i \geq 0 \\ 0 \end{cases} \quad (\text{Sign}_p(f(\cdot)_i) \lambda \geq 0)
\]

Otherwise,
\[
\frac{\varepsilon}{\Delta_p(f(\cdot)_i)} \exp^{-|\lambda|}.
\]

If the $\Delta_p(f(\cdot)_i)$ is not monotonic, then ALap is the same as the Laplace mechanism for the $i$th output. Otherwise, the distribution is the (one-sided) exponential distribution, which exhibits a smaller variance than the Laplace distribution.

**Theorem IV.4.** Given $p, \varepsilon \in \mathbb{R}^+, f : X^n \rightarrow \mathbb{R}^d$, ALap$_{p, \varepsilon, f}$ satisfies $(\varepsilon, p)$-ADP.

**Proof.** Let $M$ be ALap$_{p, \varepsilon, f}$, and assume arbitrary datasets $X$ and $X'$ such that $X \sim^p X'$. We have the following:
\[
\Pr[M(X) = (z_1, \ldots, z_d)] = \prod_{i \in [d]} \frac{\Pr[\lambda_i = z_i - f(X)_i]}{\Pr[\lambda_i = z_i - f(X')_i]} \leq \exp(\varepsilon|f(X) - f(X')|/\Delta_p(f)) \leq \exp(\varepsilon).
\]

The first inequality is from the definition of the distribution.}

**3) Utility analysis**: Assume that $\Delta_p(f)$ is monotonically decreasing. In this case, ALap$_{p, \varepsilon, f}$ uses noise following the (one-sided) exponential distribution. From this characteristic, the following two corollaries about utility can be easily derived:

**Corollary IV.5.** For all $i \in [d]$, $\mathbb{E}[|\text{ALap}_{p, \varepsilon, f}(X)_i - f(X)_i|] = \frac{\Delta_p(f)}{\varepsilon}$, where the randomness is over the mechanism.

$^3$This mechanism is a generalization of OSDPLaplace proposed by Doudalis et al. [12].
Corollary IV.6. Given dataset $X$, if $\varepsilon \geq 2\Delta(f) \log(1/(1-\beta)) / k(X)$, \text{ALap}_{p,\varepsilon,f}^\text{an} is $(p^\text{an}_f \circ f_{CT}(\cdot),\alpha,\beta)$-one-sided for all $i \in [d]$.

This phenomenon can be attributed to the output True being accurate by using $p^\text{an}_f$ as $p^\text{an}$ (i.e., outputting $p^\text{an}_f \circ \text{ALap}_{p,\varepsilon,f}$).

\text{ALap} improves the utility of the Laplace mechanism, which is two-sided and whose expected absolute error is $\sqrt{2}\Delta/\varepsilon$. Especially, Corollary IV.6 does not depend on $\alpha$. Here, \text{ALap}_{p,\varepsilon,f}^\text{an}$ is optimal with respect to one-sided error when $\Delta_p(f) = 1$ from Proposition III.4.

V. EXPERIMENTS

The source code used in these experiments is available at https://github.com/tkgsn/adp-algorithms.

A. Preliminaries

First, we detail the dataset and queries. Next, we explain the metrics to evaluate the utility of the proposed mechanisms.

1) Dataset: The real-world trajectory dataset, called Peopleflow$^4$. For simulation, we assume that data owners are infected by some disease such as COVID-19. A record (i.e., a trajectory) is a sequence of tuples $(\text{userID}, \text{latitude}, \text{longitude}, \text{placeID}, \text{state}, \text{timestamp})$: placeID represents the category of the location if the location has a category, timestamp is the times user visited the location. A total of 5,835 locations exist on Tokyo, Japan in the Peopleflow dataset, and we assume that if a tuple includes a placeID and has the “STAY” attribute, the data owner has visited the location. We specify $(3, 4, 5, 6, 7)$ as placeID, which represents shops, restaurants, entertainments, such as movie theaters and art galleries, groceries, schools, or other buildings.

2) Query: As described in Section II-B4, we queried the threshold propositions $q^\text{an}_f = p^\text{an}_f \circ f_{CT}(\cdot)$, and $q^\text{an}_f = p^\text{an}_f \circ f_{CT}(\cdot)$. Here, we explain the detail of the query. This query asks whether many people are not in close contact with each other in target locations. Thus, given target locations $(l_1, l_2, \ldots, l_d)$ and time $T$, we let $C^T = (c^1_T, c^2_T, \ldots, c^d_T)$, where $c^i_T$ is the condition that asks whether the user visited the location at time $T$. The task is to estimate the times range is very small). In this case, $f_{CT}$ is low-sensitive information because each user is able to be at only one location at time $T$. Thus, for two datasets $X, X'$ such that $X \sim X'$, $|f_{CT}(X) - f_{CT}(X')| \leq 1$.

3) Policy: Given $C^T$, we use the following policy: $p(x) := -c^1_T(x) \lor -c^2_T(x) \lor -c^d_T(x)$. Since $\Delta_p(f_{CT})$ is monotonically decreasing, \text{ALap} achieves one-sided error from Corollary IV.6 for $q^\text{an}_f$ for all $i \in [d]$. We assume that the information that a user did not visit target locations is not nonsensitive.

4) Evaluation: Given $(p^\text{an}_f \circ f_{CT}(\cdot),\alpha,\beta)$-one-sided mechanism $M$, we evaluate two types of utility: one-sided error $(1-\beta)$ and the number of locations a mechanism can answer. First, we define expected $\beta$-false as follows: given $X \in \mathbb{X}^n$,

$$\mathbb{E}[\beta \leq \ell] := \mathbb{E}_{x \sim M(X), i \in [d]}[p^\text{an}_f \circ f_{CT}(\cdot)(x)]$$

where $p^\text{an}_f$ is a $(p^\text{an}_f \circ f_{CT}(\cdot),\alpha,\beta)$-sanitizer (refer to Section II-B3). For example, if $M = \text{ALap}_{p,\varepsilon,f}$, $p^\text{an}_f(z) := p^\text{an}_f(z_i)$. Thus, $\mathbb{E}[\beta \leq \ell]$ is the expected probability that a mechanism correctly answers $q^\text{an}_f$ under the condition that $i$ is randomly selected from $[d]$ such that $q^\text{an}_f \circ f_{CT}(\cdot)(X) = \text{True}$ (i.e., condition that a target location is randomly chosen from safe locations).

Competitor: We compare the proposed mechanism with a virtual mechanism that is $(\varepsilon,\delta)$-DP and optimal.

B. Result

Here, we consider the low sensitive query by setting $T$ on an hourly basis.

1) Visualization: Here, we set $T = \text{Dec/22th/2013}$ 6 p.m. and $t = 5$, and visualized the result on Figure 2 in Introduction. Location $l_i$ is safe or dangerous if it is marked with True by a $(p^\text{an}_f \circ f_{CT}(\cdot),\alpha,\beta)$-one-sided mechanism or a $(p^\text{an}_f \circ f_{CT}(\cdot),\alpha,\beta)$-one-sided mechanism, respectively. Obscure spots represent locations where the number of visited people is obscure because of noise (one-side errors are not guaranteed). The difference is remarkable when $\alpha = 0$. 1-DP does not allow one-sided error, so all outputs are obscure. $(1,10^{-4})$-DP allows one-sided error, but almost all locations are obscure. The proposed mechanism can find 5,031 safe locations out of 5,343 locations. This phenomenon can be attributed to the relaxation by $p$.

Next, we set $\alpha = 10^{-3}$ and visualize the results on Figure 3 to show that $(\varepsilon,\delta)$-DP still miss to find many safe and dangerous locations. Here, 1-DP and $(1,10^{-4})$-DP generate almost the same results. Thus, relaxation by $\delta$ does not effectively work to achieve one-sided errors. The result of the proposed mechanism for dangerous locations are almost the same as other results because of privacy protection as presented in Section III-B2.

2) Varying parameters: We set $\varepsilon = 1$, $\alpha = 10^{-3}$, $\delta = 10^{-4}$, and $t = 5$ as default. We vary each parameter and show $\mathbb{E}[\beta \leq \ell]$ comparing with $(\varepsilon,\delta)$-DP. We randomly select $T$ and average $\mathbb{E}[\beta \leq \ell]$. The results are plotted on Figure 4.

Although $(\varepsilon,\delta)$-DP sharply decreases when $\varepsilon$ and $t$ decrease, ADP is robust to small $\varepsilon$ and small $t$. For example, in the case of $t = 1$ (i.e., judging whether one was not in close contact with an infected person), $(\varepsilon,\delta)$-DP does not work at all; by contrast, the proposed mechanism can accurately determine a not close contact condition with probability approximately 0.4.

Next, we evaluate how $\alpha$ or $\delta$ is required for $(\varepsilon,\delta)$-DP to achieve one-sided errors. ADP is not affected by $\alpha$ and $\delta$. When $\alpha = 10^{-2}$, $(\varepsilon,\delta)$-DP becomes close to ADP, but $\alpha = 10^{-2}$ is too large for our setting because if we get 5,000 answers like Figure 3 for example, it includes 50 errors in average. When $\delta = 10^{-1}$, $(\varepsilon,\delta)$-DP becomes close to ADP, $\delta = 10^{-1}$ is clearly unacceptable value.

VI. CONCLUSION

We proposed a novel privacy definition scheme, namely ADP by relaxing DP to achieve one-sided errors. We revealed

4http://pflow.csis.u-tokyo.ac.jp/
that the privacy guarantee of ADP in our case is reasonable based on Bayesian analysis. We proposed two ADP mechanisms called ALap. Finally, we conducted experiments and revealed the feasibility for epidemic surveillance using a real-world dataset.

The limitations of ADP are as follows: First, ADP results in unreasonable privacy protection to answer \( q_i \geq 1 \) with one-sided error. Second, when sensitivity is high and \( t \) and \( \varepsilon \) are small, answering many queries with practical one-sided errors becomes difficult.

This study focused on location monitoring, but one-sided errors are crucial for other subjects (e.g., outlier detection and medical care). Furthermore, ADP is the general notion of privacy; therefore, ADP effectively works more for general purposes other than one-sided errors. The results of the study can provide considerable insight for future research.

ACKNOWLEDGMENT

This work was partially supported by JST CREST JP-MJCR21M2, JST SICORP JPMISC2107, JSPS KAKENHI Grant Numbers 19H04215, 21K19767, 22H03595, 22H00521, and KDDI Foundation.

REFERENCES

[1] C. Dwork, “Differential privacy,” in Proceedings of the 33rd international conference on Automata, Languages and Programming-Volume Part II. Springer-Verlag, 2006, pp. 1–12.
[2] U. Bureau, “On the map: Longitudinal employer-household dynamics,” https://lehd.ces.census.gov/applications/help/onthemap.html#confidentiality protection,” 2020.
[3] U. Erlingsson, V. Pihur, and A. Korolova, “Rappor: Randomized aggregatable privacy-preserving ordinal response,” in Proceedings of the 2014 ACM SIGSAC conference on computer and communications security, 2014, pp. 1054–1067.
[4] A. D. P. Team, “Learning with privacy at scale,” 2017.
[5] B. Ding, J. Kulkarni, and S. Yekhanin, “Collecting telemetry data privately,” in Advances in Neural Information Processing Systems, 2017, pp. 3571–3580.
[6] N. Johnson, J. P. Near, and D. Song, “Towards practical differential privacy for sql queries,” Proceedings of the VLDB Endowment, vol. 11, no. 5, pp. 526–539, 2018.
[7] R. Kudelić, “Monte-carlo randomized algorithm for minimal feedback arc set problem,” Applied Soft Computing, vol. 41, pp. 235–246, 2016.
[8] S. Park, G. J. Choi, and H. Ko, “Information technology–based tracing strategy in response to covid-19 in south korea—privacy controversies,” Jama, 2020.
[9] C. Dwork, F. McSherry, K. Nissim, and A. Smith, “Calibrating noise to sensitivity in private data analysis,” in Theory of cryptography conference. Springer, 2006, pp. 265–284.
[10] C. Dwork and J. Lei, “Differential privacy and robust statistics,” in Proceedings of the forty-first annual ACM symposium on Theory of computing, 2009, pp. 371–380.
[11] X. He, A. Machanavajjhala, and B. Ding, “Blowfish privacy: Tuning privacy-utility trade-offs using policies,” in Proceedings of the 2014 ACM SIGMOD international conference on Management of data, 2014, pp. 1447–1458.
[12] S. Doudalis, I. Kotsogiannis, S. Haney, A. Machanavajjhala, and S. Mehrotra, “One-sided differential privacy,” ICDE, 2020.
[13] D. Kifer and A. Machanavajjhala, “Pufferfish: A framework for mathematical privacy definitions,” ACM Transactions on Database Systems (TODS), vol. 39, no. 1, pp. 1–36, 2014.
[14] M. Santha, “On the monte carlo boolean decision tree complexity of read-once formulas,” Random Structures & Algorithms, vol. 6, no. 1, pp. 75–87, 1995.
[15] A. Blum, K. Ligett, and A. Roth, “A learning theory approach to noninteractive database privacy,” Journal of the ACM (JACM), vol. 60, no. 2, pp. 1–25, 2013.