DIFFERENTIAL PRIVACY-PRESERVING NOISE ADDING MECHANISM WITH ITS APPLICATION ON CONSENSUS*

JIANPING HE†, LIN CAI‡, AND XINPING GUAN†

Abstract. Differential privacy is a formal mathematical framework for quantifying the degree of individual privacy in a statistical database. To guarantee differential privacy, a typical method is to add random noise to the original data for data release. In this paper, we investigate the conditions of differential privacy considering the general random noise adding mechanism, and then apply the obtained results for privacy analysis of the privacy-preserving consensus algorithm. Specifically, we obtain a necessary and sufficient condition of ϵ-differential privacy, and the sufficient conditions of (ϵ, δ)-differential privacy. We apply them to analyze various random noises. For the special cases with known results, our theory matches with the literature; for other cases that are unknown, our approach provides a simple and effective tool for differential privacy analysis. Applying the obtained theory on privacy-preserving consensus algorithm, we obtain the necessary condition and the sufficient condition to ensure differential privacy.

Key words. random mechanism, noise adding process, average consensus, differential privacy.

1. Introduction.

Differential privacy, a popular and widely used privacy concept, aims to minimize the chances of identifying a single record in a release of a large database [2]. Differential privacy means that the presence or absence of any individual record in the database will not affect the statistics significantly [3]. Thus, the adversary has a low chance to identify the individual's record with the released information and any auxiliary information under differential privacy. Differential privacy has been a formal framework to quantify the degree to which each individual's privacy is preserved while releasing useful statistical information about the database. We refer the readers to [4, 5] by Dwork et al. for the detailed introduction of differential privacy, including the motivation, background, the important developments of its theories and applications. More recently, Cortes et al. [6] introduced a system and control perspective on the topic of privacy-preserving data analysis, showing the importance of differential privacy in network and control area.

There are two kinds of differential privacy concepts which have been widely investigated in the literature. The first is ϵ-differential privacy. The parameter ϵ expresses the degree of the privacy protection, and a smaller value of ϵ can guarantee a stronger privacy. Based on ϵ-differential privacy, an adversary cannot gain significant information about the data function of any individual agent based on the observation of the data output. The typical approach to preserving ϵ-differential privacy is adding Laplacian noise to original data for information release. The second is (ϵ, δ)-differential privacy, which is a relaxed notion of privacy. In this privacy definition, the parameter ϵ represents the privacy degree and δ represents the probability of violating the privacy. For both parameters, smaller values correspond to higher privacy [10]. To ensure (ϵ, δ)-differential privacy, an often-used approach is adding Gaussian noise to the pure data value for query output.

Although random noise adding mechanism has been widely-used, how to design

*Part of the preliminary result of this work was presented at IEEE Conference on American Control Conference (ACC), 2017.

†Dept. of Automation, Shanghai Jiao Tong University, and Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai, China. Email: jphe@sjtu.edu.cn, xpguan@sjtu.edu.cn.

‡Dept. of Electrical & Computer Engineering at the University of Victoria, BC, Canada. Email: cai@ece.uvic.ca.

and analyze the effectiveness of various types of noises remains a challenge. Existing works mostly focused on a few well-known noise distributions (e.g., Laplacian and Gaussian). Therefore, it is worth to study the general properties of differential privacy or the basic conditions of the noise which guarantee differential privacy. Then, we can analyze the privacy of any given noise distribution and find the best noise distribution in terms of the degree of the privacy protection. To fill this gap, in this paper, we first investigate the basic conditions for the random noise adding mechanism, under which differential privacy can be guaranteed. We then obtain the conditions to determine whether the differential privacy is guaranteed by the noise adding mechanism. To show this statement, we analyze the well-known noise adding mechanisms, e.g., Laplacian and Gaussian. For the special cases with known results, our theory matches with the literature; for other cases that are unknown, our approach provides a simple and effective tool for differential privacy analysis. In addition, we apply the theory to analyze the privacy of the privacy-preserving consensus algorithms, a hot topic in the control and optimization area recently, and obtain the necessary condition and the sufficient condition to ensure differential privacy. The main contributions of this paper are summarized as follows.

- We investigate the conditions of a general random noise adding mechanism to guarantee differential privacy. We obtain a necessary and sufficient condition of ϵ-differential privacy, and the sufficient conditions of (ϵ, δ)-differential privacy. Meanwhile, we provide the computation approach to estimate the values of ϵ and δ, respectively.
- We show that the obtained theory provides an efficient and simple approach for the analysis of both ϵ-differential privacy and (ϵ, δ)-differential privacy. Using the obtained results, it is easy to obtain the properties of differential privacy for any adding noise when its probability density function is given.
- We apply the theorems of differential privacy to analyze the privacy of general privacy-preserving consensus algorithm. We obtain the necessary condition and the sufficient condition for the algorithm under which differential privacy is achieved. Based on these conditions, the privacy of existing privacy-preserving consensus algorithms is analyzed. Also, it is proved that achieving the average consensus and ϵ-differential privacy simultaneously is impossible.

Different from the existing work, we obtain more general properties and conditions of differential privacy mathematically, and the proposed results can be used to analyze the privacy property of the random noise adding mechanism with any noise distributions.

The remainder of this paper is organized as follows. The related works are given in Section 2. Section 3 formulates the problem. In Section 4, we provide the basic theoretical results of differential privacy. Section 5 studies the application on privacy-preserving consensus algorithm. Conclusions are summarized in Section 6.

2. Related Works. The concept of differential privacy (including ϵ-differential privacy and (ϵ, δ)-differential privacy) was first introduced by Dwork et al. [2,4]. Since then, differential privacy has attracted substantial attention throughout computer science, control and communication communities, including areas like deep learning [9], optimization [8, 25], dynamic systems [22] and more. There are also some other privacy definitions, e.g., identifiability and mutual-information privacy, and we refer the readers to [32] for the relationship among these privacy concepts.

Dwork et al. [2] showed that the Laplacian mechanism, i.e., adding random noise with Laplace distribution proportional to the global sensitivity of the query function

to perturb the query output, can preserve ϵ-differential privacy. Also, it was shown that the exponential mechanism [11] and staircase mechanism [12] can preserve ϵ-differential privacy for general query functions. It was shown that adding random noise with Gaussian distribution can preserve the (ϵ, δ)-differential privacy for both real valued query functions [4] and infinite dimensional query functions [13]. For the work on enforcing differential privacy in optimization, linear programs are solved in a framework that allows for keeping objective functions or constraints private [7]. This work was extended by the authors of [8], and they considered a similar setting wherein some affine objectives with linearly constrained problems are solved while keeping the privacy of the objective functions. To keep inputs private from an adversary observing a system's outputs, differential privacy has been adapted to dynamical systems, which introduces the privacy concerns in the context of systems theory [22]. Wasserman and Zhou in [30] proposed a statistical framework for differential privacy, where the differential privacy is investigated from a statistical perspective. Nissim et al. in [33] introduced a new generic framework for private data analysis, which allows one to release functions f of the data with instance-specific additive noise.

Recently, privacy issues are concerned in multi-agent systems, and mainly investigating the privacy-preserving consensus problem. The objective is to guarantee that the agents' initial states (or objective functions) are private and the average consensus is achieved [22, 24–28]. In [25], the authors solved distributed consensus problems while keeping the agents' objective functions private, and in [24] the same authors solved similar problems while keeping the privacy of each agent's initial state. In these works, differential privacy is guaranteed by adding independent and Laplacian noises to the consensus process. More recently, Nozari et al. [26] obtained and proved an interesting impossibility result that achieving average consensus and differential privacy simultaneously is impossible by contradiction via the definition of differential privacy. This result is also proved in this paper by comparing the necessary conditions of differential privacy and of the average consensus.

Different from the existing work, in this paper, we obtain a necessary and sufficient condition of ϵ-differential privacy, and the sufficient conditions of (ϵ, δ)-differential privacy. Thus, more general properties of differential privacy are obtained, and they can be used to analyze the random noise adding mechanism with any distribution.

3. Preliminary and Problem Formulation.

3.1. Preliminary. Let $V = \{1, 2, ..., n\}$ be the set of nodes (users). Following [23–26], we define σ-adjacency and differential privacy, respectively, as follows.

DEFINITION 3.1 (σ-adjacency). *Given $\sigma \in \mathbf{R}^+$, the state vector x and y are σ-adjacent if, for some $i_0 \in V$,*

$$|x_i - y_i| \leq \begin{cases} \sigma, & \text{if } i = i_0; \\ 0, & \text{if } i \neq i_0, \end{cases} \tag{3.1}$$

for $i \in V$, where $x, y \in \mathbf{R}^n$.

From the above definition, it follows that a pair of σ-adjacent vectors x and y have at most one different element, and the difference is no more than σ. For example, $x = [0, 1]$ and $y = [1, 1]$ are 1-adjacent vectors.

DEFINITION 3.2 ((ϵ, δ)-differential privacy). *A randomized mechanism $\mathcal{A}$ with domain Ω is (ϵ, δ)-differentially private if, for any pair x and y ($x, y \in \Omega$) of σ-adjacent state vector and any set $\mathcal{O} \subseteq Range(\mathcal{A})$, where $Range(\mathcal{A})$ is the domain of*

the output under mechanism $\mathcal{A}$*,*

$$\Pr\{\mathcal{A}(x) \in \mathcal{O}\} \leq e^{\epsilon} \Pr\{\mathcal{A}(y) \in \mathcal{O}\} + \delta. \tag{3.2}$$

In the above privacy definition, there are two key parameters, ϵ and δ, which represent the privacy cost and the probability of violating the privacy cost, respectively. For both of these parameters, smaller values imply stronger privacy guarantees. If $\delta = 0$, we say that $\mathcal{A}$ is ϵ-differentially private, which provides a stronger privacy than (ϵ, δ)-differential privacy.

Table 3.1 summarizes a few important notations in this paper for easy reference.

TABLE 3.1
Important Notations

Symbol	Definition
x, y	a pair of σ-adjacent n dimensional vector
$\mathcal{A}$	a random mechanism
σ	a parameter expressing the adjacency between vectors
ϵ	a parameter expressing the privacy cost
δ	a parameter expressing the probability of the violating the privacy
$\mathcal{O}$	a subset of Range($\mathcal{A}$)
$\mathcal{O}_i$	the set of i-th column element of $\mathcal{O}$
Range($\mathcal{A}$)	the domain of the output under mechanism $\mathcal{A}$
$f_{\theta_i}(z)$	the probability density function of random variable θ_i
μ	the function of Lebesgue measure
Φ_i^0	the zero point set of the function $f_{\theta_i}(z)$
W	the weight matrix in a consensus alogrithm
$\bar{x}$	the average value of all node states

3.2. Problem Formulation. General Random Mechanism: We consider a general random noise adding mechanism. Assume that the randomized mechanism $\mathcal{A} : \Omega \to \text{Range}(\mathcal{A})$ satisfies

$$\mathcal{A}(x) = x + \theta, \ \forall \ x \in \Omega, \tag{3.3}$$

where $\theta \in \Theta$ is a random noise vector with $f_{\theta_i}(z)$ as the PDF of its i-th element θ_i, and $\Theta \subseteq R^n$. We assume that each $f_{\theta_i}(z)$ is a continuous or piecewise continuous function, and θ_i and θ_j are independent from each other for $\forall i \neq j$ (each node in a network adds the noise by itself in application). Then, we have Range($\mathcal{A}$) $= \Omega \oplus \Theta$, where $\oplus$ denotes the Minkowski sum between two set, i.e., any element in Range($\mathcal{A}$) will equal to the sum of two elements in sets Ω and Θ. The random mechanism $\mathcal{A}$ defined in (3.3) is a general noise adding mechanism, where x could be substituted by a general invertible function of x with Lipschitz condition and θ could also be a function of random variables[1].

[1]For example, we consider a more general mechanism as follows

$$\mathcal{A}(x) = g(x) + h(\theta), \ \forall \ x \in \Omega, \theta \in \Theta,$$

where $g(x)$ is a function of x satisfying $|g(x) - g(y)| \leq L|x - y|$ (where L is a Lipschitz constant) and $g(x) \neq g(y)$ when $x \neq y$ and $h(\theta)$ is a function of θ. We can use the similar analytical approach given in this paper to analyze differential privacy of the above mechanism.

Problem of Interests: The goal of this paper is to investigate the following two issues: i) what are general properties of differential privacy considering (3.3), i.e., what kinds of conditions (e.g., the sufficient and necessary conditions of differential privacy) can guarantee the differential privacy of the randomized mechanism $\mathcal{A}$. For example, if the adding noise in (3.3) follows the following distribution,

$$f_{\theta_i}(z) = \begin{cases} \frac{z}{2}e^{-z}, & z \geq 0; \\ \frac{-z}{2}e^{z}, & z \leq 0, \end{cases} \tag{3.4}$$

how can we quickly know whether $\mathcal{A}$ achieves ϵ-differential privacy or not. ii) How to extend and apply the obtained results for privacy analysis on the privacy-preserving consensus algorithm, an important distributed iterative algorithm in the control area. We solve these two problems in the following two sections, respectively.

4. Conditions of Differential Privacy. In this section, the basic conditions of differential privacy considering $\mathcal{A}$ defined in (3.3) are obtained first, followed by the estimations of the privacy parameters. Then, we show that the obtained conditions provide efficient criteria of differential privacy through case studies, where the Laplacian, Gaussian, and Uniform noises are investigated, by using the developed theoretical results. In the remainder part of this paper, we let $\frac{\{\cdot\}}{0} = \infty$ for any $\{\cdot\} \neq 0$.

4.1. Necessary and Sufficient Condition. In this subsection, considering the mechanism $\mathcal{A}$, we give a necessary and sufficient condition of ϵ-differentially private in the following theorem.

THEOREM 4.1. *$\mathcal{A}$ is ϵ-differentially private if and only if (iff) the following two conditions hold,*

c_1: zero measure of the zero-point set, i.e.,

$$\mu\left(\cup_{i=1}^{n}\Phi_i^0\right) = 0 \tag{4.1}$$

where $\Phi_i^0 = \{z | f_{\theta_i}(z) = 0, z \in \mathbf{R}\}$ is the zero point set and $\mu(\cdot)$ is the Lebesgue measure;

c_2: there exists a positive constant c_b such that

$$\sup_{\hat{\sigma}\in[-\sigma,\sigma], f_{\theta_i}(z)\neq 0} \frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)} = c_b, \tag{4.2}$$

for $\forall i \in V$, where the acnodes' space (isolated point set) of $f_{\theta_i}(z)$ is not considered,

where $\epsilon = \log(c_b)$, and c_b is an increasing function of σ.

Proof. $\Leftarrow$: We prove the necessity by contradiction.

First, we prove that (4.1) is a necessary condition. Assume that $\mu\left(\cup_{i=1}^{n}\Phi_i^0\right) > 0$, which means that there exists at least one $i_0 \in V$ with $\mu\left(\Phi_{i_0}^0\right) > 0$. Thus, there exists a continuous interval $[a, b]$ such that

$$f_{\theta_{i_0}}(z) = 0, \ \forall \ z \in [a, b], \tag{4.3}$$

and

$$f_{\theta_{i_0}}(z) > 0, \ \text{for } z > b, \tag{4.4}$$

or $f_{\theta_{i_0}}(z) > 0$ for $z < a$ [2].

[2]Without loss of generality, suppose $f_{\theta_i}(z) > 0$ holds for $z > b$ in the following proof.

For σ-adjacent state vectors x and y, we let $x_{i_0} = y_{i_0} - \sigma$ and $x_i = y_i$ (when $i \neq i_0$), where $\sigma < b - a$. Then, with (3.3), we have $\mathcal{A}(x_{i_0}) = x_{i_0} + \theta$ and $\mathcal{A}(y_{i_0}) = y_{i_0} + \theta$. Define a subset $\mathcal{O}_{i_0} = [y_{i_0} + a, y_{i_0} + b]$, which satisfies $\mathcal{O}_{i_0} \subseteq \text{Range}(\mathcal{A}(x_{i_0}))$. From (4.3) and (4.4), it follows that

$$\begin{aligned}
&\Pr\{\mathcal{A}(x_{i_0}) \in \mathcal{O}_{i_0}\} = \int_{y_{i_0}+a}^{y_{i_0}+b} f_{x_{i_0}+\theta_{i_0}}(z)\mathrm{d}z \\
&= \int_{y_{i_0}+a-x_{i_0}}^{y_{i_0}+b-x_{i_0}} f_{\theta_{i_0}}(z)\mathrm{d}z = \int_{a+\sigma}^{b+\sigma} f_{\theta_{i_0}}(z)\mathrm{d}z \\
&= \int_{a+\sigma}^{b} f_{\theta_{i_0}}(z)\mathrm{d}z + \int_{b}^{b+\sigma} f_{\theta_{i_0}}(z)\mathrm{d}z \\
&= \int_{b}^{b+\sigma} f_{\theta_{i_0}}(z)\mathrm{d}z > 0,
\end{aligned}$$

while

$$\begin{aligned}
\Pr\{\mathcal{A}(y_{i_0}) \in \mathcal{O}_{i_0}\} &= \int_{y_{i_0}+a}^{y_{i_0}+b} f_{y_{i_0}+\theta_{i_0}}(z)\mathrm{d}z \\
&= \int_{a}^{b} f_{\theta_{i_0}}(z)\mathrm{d}z = 0.
\end{aligned}$$

Hence, it follows that

$$\begin{aligned}
&\frac{\Pr\{\mathcal{A}(x) \in \mathcal{O}\}}{\Pr\{\mathcal{A}(y) \in \mathcal{O}\}} \\
=&\frac{\Pr\{\mathcal{A}(x_{i_0}) \in \mathcal{O}_{i_0}\}\prod_{i=1,i\neq i_0}^{n}\Pr\{\mathcal{A}(x_i) \in \mathcal{O}_i\}}{\Pr\{\mathcal{A}(y_{i_0}) \in \mathcal{O}_{i_0}\}\prod_{i=1,i\neq i_0}^{n}\Pr\{\mathcal{A}(y_i) \in \mathcal{O}_i\}} \\
=&\frac{\Pr\{\mathcal{A}(x_{i_0}) \in \mathcal{O}_{i_0}\}}{\Pr\{\mathcal{A}(y_{i_0}) \in \mathcal{O}_{i_0}\}} = \infty,
\end{aligned} \tag{4.5}$$

where $\mathcal{O}_i$ is the domain of the i-th element in $\mathcal{O}$. It contradicts with the definition of ϵ-differential privacy. Thus, one obtains that (4.1) is a necessary condition if $\mathcal{A}$ is ϵ-differentially private.

Second, we prove that (4.2) is also a necessary condition. Suppose that

$$\sup_{\hat{\sigma}\in[-\sigma,\sigma], f_{\theta_i}(z)\neq 0} \frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)} = \infty.$$

Then, for any given large constant M, there exist z_0 and $\hat{\sigma} \in [-\sigma, \sigma]$ such that $f_{\theta_i}(z_0) \neq 0$ and

$$\frac{f_{\theta_i}(z_0 + \hat{\sigma})}{f_{\theta_i}(z_0)} \geq M.$$

Since (4.1) holds and the measure of the acnodes is also zero, we can ignore these two cases when we calculate the probability. We thus assume that $f_{\theta_{i_0}}(z)$ is a continuous function in a small interval around z_0 and around $z_0 + \hat{\sigma}$. Then, we have that there exists a small positive constant ε_0 such that

$$\max_{z\in[z_0,z_0+\varepsilon_0]} f_{\theta_{i_0}}(z) \leq 2 f_{\theta_i}(z_0)$$

and

$$\min_{z\in[z_0+\hat{\sigma},z_0+\hat{\sigma}+\varepsilon_0]} f_{\theta_{i_0}}(z) \geq (M-1) f_{\theta_i}(z_0).$$

Then, we construct a pair of $\hat{\sigma}$-adjacent state vector x and y with $x_{i_0} = y_{i_0} - \hat{\sigma}$ and $x_i = y_i$ (when $i \neq i_0$). Define the set $\mathcal{O}_{i_0}^0 = [y_{i_0} + z_0, y_{i_0} + z_0 + \varepsilon_0]$, where $\varepsilon_0 \leq \hat{\sigma}$. Based on (3.3), we have

$$\begin{aligned}
\frac{\Pr\{\mathcal{A}(x_{i_0}) \in \mathcal{O}_{i_0}^0\}}{\Pr\{\mathcal{A}(y_{i_0}) \in \mathcal{O}_{i_0}^0\}} &= \frac{\int_{y_{i_0}+z_0}^{y_{i_0}+z_0+\varepsilon_0} f_{x_{i_0}+\theta_{i_0}}(z)\mathrm{d}z}{\int_{y_{i_0}+z_0}^{y_{i_0}+z_0+\varepsilon_0} f_{y_{i_0}+\theta_{i_0}}(z)\mathrm{d}z} \\
&= \frac{\int_{z_0+\hat{\sigma}}^{z_0+\hat{\sigma}+\varepsilon_0} f_{\theta_{i_0}}(z)\mathrm{d}z}{\int_{z_0}^{z_0+\varepsilon_0} f_{\theta_{i_0}}(z)\mathrm{d}z} \\
&\geq \frac{(M-1) f_{\theta_i}(z_0)\varepsilon_0}{2 f_{\theta_i}(z_0)\varepsilon_0} \\
&\geq \frac{(M-1)}{2}.
\end{aligned}$$

Then, similar to (4.5), we infer that

$$\frac{\Pr\{\mathcal{A}(x) \in \mathcal{O}\}}{\Pr\{\mathcal{A}(y) \in \mathcal{O}\}} \geq \frac{(M-1)}{2}.$$

Note that M could be an arbitrarily large constant, which implies that $\mathcal{A}$ is not ϵ-differentially private. Hence, (4.10) is also a necessary condition to ensure that $\mathcal{A}$ is ϵ-differentially private.

$\Rightarrow$: Next, we prove the sufficiency. Since (4.1) holds, the cases that $f_{\theta_i}(z) = 0, \forall i \in V$ and the acnodes are ignored when we calculate a probability. Let $\mathcal{O}_i$ be the domain/set of i-th element in $\mathcal{O}$ for $l = 1, ..., n$. Under (3.3), we have

$$\begin{aligned}
&\Pr\{\mathcal{A}(x) \in \mathcal{O}\} = \Pr\{x + \theta \in \mathcal{O}\} \\
&= \Pr\{x_{i_0} + \theta_{i_0} \in \mathcal{O}_{i_0}\} \prod_{i=1, i\neq i_0}^{n} \Pr\{x_i + \theta_i \in \mathcal{O}_i\}
\end{aligned} \tag{4.6}$$

and

$$\begin{aligned}
&\Pr\{\mathcal{A}(y) \in \mathcal{O}\} = \Pr\{y + \theta \in \mathcal{O}\} \\
&= \Pr\{y_{i_0} + \theta_{i_0} \in \mathcal{O}_{i_0}\} \prod_{i=1, i\neq i_0}^{n} \Pr\{y_i + \theta_i \in \mathcal{O}_i\}.
\end{aligned} \tag{4.7}$$

Since $x_i = y_i, i \neq i_0$, we have

$$\prod_{i=1, i\neq i_0}^{n} \Pr\{x_i + \theta_i \in \mathcal{O}_i\} = \prod_{i=1, i\neq i_0}^{n} \Pr\{y_i + \theta_i \in \mathcal{O}_i\}. \tag{4.8}$$

Meanwhile, with the condition c_2, it follows

$$\begin{aligned}
&\Pr\{x_{i_0} + \theta_{i_0} \in \mathcal{O}_{i_0}\} = \oint_{\mathcal{O}_{i_0}} f_{x_{i_0}+\theta_{i_0}}(z)\mathrm{d}z \\
&= \oint_{\mathcal{O}_{i_0}} f_{y_{i_0}-\hat{\sigma}+\theta_{i_0}}(z)\mathrm{d}z \leq \oint_{\mathcal{O}_{i_0}} c_b f_{y_{i_0}+\theta_{i_0}}(z)\mathrm{d}z \\
&= c_b \Pr\{y_{i_0} + \theta_{i_0} \in \mathcal{O}_{i_0}\},
\end{aligned} \tag{4.9}$$

where we have used (4.2). Substituting (4.8) and (4.9) into (4.6) yields

$$\begin{aligned}\Pr\{\mathcal{A}(x) \in \mathcal{O}\} &\leq c_b \Pr\{\mathcal{A}(y) \in \mathcal{O}\} \\ &= e^{\log(c_b)} \Pr\{\mathcal{A}(y) \in \mathcal{O}\}.\end{aligned}$$

Thus, $\mathcal{A}$ is ϵ-differentially private with $\epsilon = \log(c_b)$. Note that in condition c_2, the bound c_b depends on the adjacency parameter σ, and clearly we have

$$\sup_{\hat{\sigma}\in[-\sigma_1,\sigma_1], f_{\theta_i}(z)\neq 0} \frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)} \leq \sup_{\hat{\sigma}\in[-\sigma_2,\sigma_2], f_{\theta_i}(z)\neq 0} \frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)}$$

holds for $\sigma_1 \leq \sigma_2$. It implies that c_b is an increasing function of σ. □

The above theorem indicates a relationship among ϵ, σ and ϵ. Since a smaller ϵ provides a stronger privacy guarantee, it shows that $\epsilon \to 0$ if $c_b \to 1$, i.e., a stronger privacy can be guaranteed when c_b becomes smaller. Then, we have that

$$\begin{aligned}&\sup_{\hat{\sigma}\in[-\sigma,\sigma], f_{\theta_i}(z)\neq 0} \frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)} = c_b \\ \Leftrightarrow &\sup_{\hat{\sigma}\in[-\sigma,\sigma], f_{\theta_i}(z)\neq 0} \log(f_{\theta_i+\hat{\sigma}}(z)) - \log(f_{\theta_i}(z)) = \log(c_b)\end{aligned}$$

Thus, the condition c_2 in Theorem 4.1 is equivalent to the following condition,

c_2': $\log(f_{\theta_i}(z))$ is a uniformly bounded function for $\forall i \in V$ and $f_{\theta_i}(z) \neq 0$. When the changing interval size of the variable z is no more than σ, the upper bounded of all $\log(f_{\theta_i}(z))$ for $\forall i \in V$ and $f_{\theta_i}(z) \neq 0$, is $\log(c_b)$.

The proof is straightforward to obtain, so it is omitted here. Therefore, c_2' can be used to easily determine whether c_2 is true or not.

It is well known that a smaller ϵ provides a stronger privacy guarantee. Can we find a noise distribution such that $\mathcal{A}$ is ϵ-differentially private for any small ϵ? Based on the above theoretical results, we will find a random distribution which can guarantee any small ϵ-differential private. From the above corollary, we note that $\epsilon \to 0$ if $c_b \to 1$, i.e., a stronger privacy can be guaranteed when c_b becomes smaller. For any $c_b > 1$, we construct a staircase-shaped PDF for each random variable used the noise adding mechanism, such that the conditions c_1 and c_2 can be satisfied. The PDF is given by

$$f(z) = \begin{cases} \dfrac{1-\varrho}{2a}\varrho^k, & z \in [ka, (k+1)a]; \\ \dfrac{1-\varrho}{2a}, & z \in [-a, a]; \\ \dfrac{1-\varrho}{2a}\varrho^k, & z \in [-ka-a, -ka], \end{cases}$$

where $\varrho \in (0, 1)$ and k is a positive integer and a is a positive constant. A staircase-shaped PDF is shown in Fig. 4.1. For the above staircase-shaped function $f(z)$, we obtain that

$$\int_{-\infty}^{+\infty} f(z)\mathrm{d}z = (1-\varrho) + 2\sum_{k=1}^{\infty} \frac{1-\varrho}{2}\varrho^k = 1,$$

and thus it is a PDF function for a random variable. In this case, when $\sigma \leq 1$, it follows that

$$\sup_{\hat{\sigma}\in[-\sigma,\sigma], f_{\theta_i}(z)\neq 0} \frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)} = \frac{1}{\varrho},$$

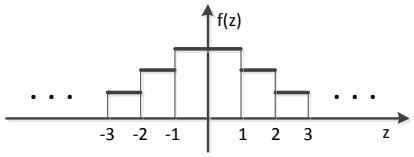

FIG. 4.1. *The staircase-shaped PDF guarantees that $\mathcal{A}$ is $\log(\frac{1}{\varrho})$-differentially private.*

which ensures that $\mathcal{A}$ is $\log(\frac{1}{\varrho})$-differentially private. Note that ϱ could be any value in $(0,1)$, which means that c_b could be any value in $(1,\infty)$ by setting $\varrho = \frac{1}{c_b}$. Hence, for any small $\epsilon > 0$, we can find a staircase-shaped PDF for the adding noise such that $\mathcal{A}$ is ϵ-differentially private.

Next, we provide another necessary condition and sufficient condition of ϵ-differentially private, respectively.

THEOREM 4.2. *If $\mathcal{A}$ is ϵ-differentially private, then $\forall i \in V$, there $\nexists\ c_o \in (-\infty,+\infty)$, such that*

$$\lim_{z\to c_0} f_{\theta_i}(z) = 0. \tag{4.10}$$

Proof. Suppose that there exists a bounded constant $c_0 \in (-\infty,+\infty)$, such that $\lim_{z\to c_0} f_{\theta_{i_0}}(z) = 0$. Since (4.1) holds, we can set $f_{\theta_{i_0}}(c_0) = 0$ and suppose that $f_{\theta_{i_0}}(z)$ is a continuous function in a small interval around c_0. Then, there exists an interval $[c_0, c_1]$ and a small $\hat{\sigma} \le \frac{c_1-c_0}{2}$ such that

$$\max_{z\in[c_0,c_0+\hat{\sigma}]} f_{\theta_{i_0}}(z) \le \hat{\epsilon}(\hat{\sigma})$$

and

$$\max_{z\in[c_0+\hat{\sigma},c_1]} f_{\theta_{i_0}}(z) > \hat{\epsilon}(\hat{\sigma})$$

where $\hat{\epsilon}(\hat{\sigma})$ satisfies $\lim_{\hat{\sigma}\to 0}\hat{\epsilon}(\hat{\sigma}) = 0$. Then, we construct a pair of $\hat{\sigma}$-adjacent state vector x and y with $x_{i_0} = y_{i_0} - \hat{\sigma}$ and $x_i = y_i$ (when $i \neq i_0$). Define the set $\mathcal{O}_{i_0}^k = [y_{i_0} + c_0, y_{i_0} + c_0 + \hat{\sigma}(k)]$, where $\hat{\sigma}(k) \le \hat{\sigma}$. Based on (3.3), we have

$$\begin{aligned}
\frac{\Pr\{\mathcal{A}(x_{i_0}) \in \mathcal{O}_{i_0}^k\}}{\Pr\{\mathcal{A}(y_{i_0}) \in \mathcal{O}_{i_0}^k\}} &= \frac{\int_{y_{i_0}+c_0}^{y_{i_0}+c_0+\hat{\sigma}(k)} f_{x_{i_0}+\theta_{i_0}}(z)\mathrm{d}z}{\int_{y_{i_0}+c_0}^{y_{i_0}+c_0+\hat{\sigma}(k)} f_{y_{i_0}+\theta_{i_0}}(z)\mathrm{d}z} \\
&= \frac{\int_{c_0+\hat{\sigma}}^{c_0+\hat{\sigma}+\hat{\sigma}(k)} f_{\theta_{i_0}}(z)\mathrm{d}z}{\int_{c_0}^{c_0+\hat{\sigma}(k)} f_{\theta_{i_0}}(z)\mathrm{d}z} \\
&\ge \frac{\hat{\epsilon}(\hat{\sigma})\hat{\sigma}(k)}{\hat{\epsilon}(\hat{\sigma}(k))\hat{\sigma}(k)} \ge \frac{\hat{\epsilon}(\hat{\sigma})}{\hat{\epsilon}(\hat{\sigma}(k))}.
\end{aligned}$$

Let $\hat{\sigma}(k) \to 0$, one obtains

$$\lim_{\hat{\sigma}(k)\to 0} \frac{\Pr\{\mathcal{A}(x_{i_0}) \in \mathcal{O}_{i_0}^k\}}{\Pr\{\mathcal{A}(y_{i_0}) \in \mathcal{O}_{i_0}^k\}} \ge \lim_{\hat{\sigma}(k)\to 0} \frac{\hat{\epsilon}(\hat{\sigma})}{\hat{\epsilon}(\hat{\sigma}(k))} = +\infty,$$

which implies that $\mathcal{A}$ is not ϵ-differentially private. It leads to a contradiction. Thus, (4.10) is a necessary condition when $\mathcal{A}$ is ϵ-differentially private, which completes the proof. □

(4.10) is actually a necessary condition of c_2, which can be easily proved by contradiction. This further explains why (4.10) is necessary to ϵ-differential privacy.

THEOREM 4.3. *$\mathcal{A}$ is ϵ-differentially private with $\epsilon = \log(c_b)$, if, $\forall i \in V$, there exists a positive constant c_b such that*

$$\sup_{\hat{\sigma}\in[-\sigma,\sigma]} \frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)} = c_b. \tag{4.11}$$

Proof. Note that if (4.11) can guarantee both conditions c_1 and c_2, then this theorem can be proved from Theorem 4.1.

First, we prove that (4.11) guarantees condition c_2. By comparing (4.2) and (4.11), we note that the constraint $f_{\theta_i}(z) \neq 0$ in (4.2) is removed in (4.11), which means that (4.11) provides a more general result than (4.2). Hence, one infers that condition c_2 is guaranteed by (4.11) directly.

Then, we prove that (4.11) can also guarantee condition c_1. First, suppose that c_1 is not true, then there exists a continuous interval such that $f_{\theta_i}(z) = 0$ for z in this interval. Second, since $f_{\theta_i}(z)$ is a PDF of a random variable, we have $f_{\theta_i}(z) \geq 0$ and $\int_{-\infty}^{\infty} f_{\theta_i}(z)\mathrm{d}z = 1$. Thus, there exists a continuous interval such that $f_{\theta_i}(z) > 0$ holds in this interval. Then, we further infer that there exist two continuous intervals (a, b) and (b, c) such that $f_{\theta_i}(z) = 0$ for $z \in (a, b)$ and $f_{\theta_i}(z) > 0$ for $z \in (b, c)$. It means that

$$\sup_{\hat{\sigma}\in[-\sigma,\sigma]} \frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)} \geq \sup_{\hat{\sigma}\in[-\sigma,\sigma]} \frac{f_{\theta_i}(b+\frac{\hat{\sigma}}{2})}{f_{\theta_i}(b-\frac{\hat{\sigma}}{2})} = \infty, \tag{4.12}$$

which leads to a contradiction. Therefore, we have that c_1 is also true under (4.11).

We thus have completed the proof. □

From the above proof, we know that (4.11) is a stronger condition than conditions c_1 and c_2. Thus, (4.11) is a sufficient but not necessary condition.

4.2. Sufficient Condition for (ϵ, δ)-Differential Privacy. In this subsection, we study the relaxed differential privacy, named (ϵ, δ)-differential privacy. We obtain the sufficient conditions to guarantee that $\mathcal{A}$ provides (ϵ, δ)-differential privacy, followed by the estimations of both the parameters ϵ and δ.

THEOREM 4.4. *If (4.2) holds, then $\mathcal{A}$ is (ϵ, δ)-differentially private, where ϵ and δ satisfy $\epsilon = \log(c_b)$ and*

$$\delta = \max_{i\in V} \oint_{\Phi_i^0} f_{\theta_i}(z+\sigma)dz. \tag{4.13}$$

Moreover, if (4.1) holds, we have $\delta = 0$, i.e., $\mathcal{A}$ is ϵ-differentially private.

Proof. Similarly, assume the σ-Adjacency state vectors x and y satisfy $y_{i_0} = x_{i_0} + \sigma$ and $x_i = y_i, i \neq i_0$, and define $\mathcal{O}_l$ to be the l-th column element of $\mathcal{O}$ for $l = 1, ..., n$. Then, we have that (4.6), (4.7) and (4.8) still hold true.

First, we consider the case that $\mu(\cup_{i\in V}\Phi_i^0) > 0$. Given the non-zero measure of

the zero point set, (4.9) no longer holds true but we can obtain the following result,

$$\begin{aligned}
&\Pr\{x_{i_0}+\theta_{i_0}\in\mathcal{O}_{i_0}\}=\oint_{\mathcal{O}_{i_0}} f_{x_{i_0}+\theta_{i_0}}(z)\mathrm{d}z\\
&=\oint_{\mathcal{O}_{i_0}} f_{y_{i_0}-\sigma+\theta_{i_0}}(z)\mathrm{d}z\le\oint_{\mathcal{O}_{i_0}} c_b f_{y_{i_0}+\theta_{i_0}}(z)\mathrm{d}z\\
&+\oint_{\{\Phi_{i_0}^0+y_{i_0}\}\cap\mathcal{O}_{i_0}} f_{y_{i_0}-\sigma+\theta_{i_0}}(z)\mathrm{d}z\\
&\le c_b\Pr\{y_{i_0}+\theta_{i_0}\in\mathcal{O}_{i_0}\}+\oint_{\{\Phi_{i_0}^0+y_{i_0}\}} f_{y_{i_0}-\sigma+\theta_{i_0}}(z)\mathrm{d}z\\
&\le c_b\Pr\{y_{i_0}+\theta_{i_0}\in\mathcal{O}_{i_0}\}+\oint_{\Phi_{i_0}^0} f_{\theta_{i_0}}(z+\sigma)\mathrm{d}z, \qquad (4.14)
\end{aligned}$$

where we have used the fact that $f_{\theta_{i_0}-\sigma}(z)=f_{\theta_{i_0}}(z+\sigma)$. Then, one infers from (4.6), (4.7), (4.8) and (4.14) that

$$\begin{aligned}
\Pr\{\mathcal{A}(x)\in\mathcal{O}\}&=\prod_{l=1}^n\Pr\{\mathcal{A}(x_l)\in\mathcal{O}_l\}\\
&=\Pr\{\mathcal{A}(x_{i_0})\in\mathcal{O}_{i_0}\}\prod_{l=1,l\neq i_0}^n\Pr\{\mathcal{A}(x_l)\in\mathcal{O}_l\}\\
&\le c_b\Pr\{\mathcal{A}(y_{i_0})\in\mathcal{O}_{i_0}\}\prod_{l=1,l\neq i_0}^n\Pr\{\mathcal{A}(y_l)\in\mathcal{O}_l\}\\
&\quad+\oint_{\Phi_{i_0}^0} f_{\theta_{i_0}}(z+\sigma)\mathrm{d}z\prod_{l=1,l\neq i_0}^n\Pr\{\mathcal{A}(y_l)\in\mathcal{O}_l\}\\
&\le c_b\Pr\{\mathcal{A}(y)\in\mathcal{O}\}+\max_{i\in V}\oint_{\Phi_i^0} f_{\theta_i}(z+\sigma)\mathrm{d}z,
\end{aligned}$$

which means that $\mathcal{A}$ is (ϵ,δ)-differentially private.

Next, if $\mu(\cup_{i\in V}\Phi_i^0)=0$, we have that $\mu(\Phi_i^0)=0$ holds for $\forall i\in V$. Then, we obtain that

$$\delta=\max_{i\in V}\oint_{\Phi_i^0} f_{\theta_i}(z+\sigma)\mathrm{d}z=0,$$

i.e., $\mathcal{A}$ is ϵ-differentially private. □

In the above theorem, note that

$$\begin{aligned}
&\oint_{\Phi_i^0} f_{\theta_i}(z+\sigma)\mathrm{d}z\le\oint_{\Phi_i^0\cap\{\mathbf{R}-\{\Phi_i^0+\sigma\}\}} f_{\theta_i}(z+\sigma)\mathrm{d}z\\
&\le\max_{\Phi\subset\mathbf{R},\mu(\Phi)=\mu(\Phi_i^0\cap\{\mathbf{R}-\{\Phi_i^0+\sigma\}\})}\oint_{\Phi} f_{\theta_i}(z)\mathrm{d}z.
\end{aligned}$$

It means that δ satisfies

$$\begin{aligned}
\delta&\le\max_{\Phi\subset\mathbf{R},\mu(\Phi)=\mu(\Phi_i^0\cap\{\mathbf{R}-\{\Phi_i^0+\sigma\}\}),i\in V}\oint_{\Phi} f_{\theta_i}(z)\mathrm{d}z\\
&\le\max_{i\in V}\left[\mu(\Phi_i^0\cap\{\mathbf{R}-\{\Phi_i^0+\sigma\}\})\sup_{z\in\mathbf{R}} f_{\theta_i}(z)\right]. \qquad (4.15)
\end{aligned}$$

Meanwhile, we have

$$\lim_{\sigma\to 0}\mu(\Phi_i^0\cap\{\mathbf{R}-\{\Phi_i^0+\sigma\}\})=0.$$

Hence, when the PDF of the adding noise is given, we have

$$\lim_{\sigma\to 0}\delta=0,$$

i.e., smaller σ-adjacency vectors can guarantee a smaller δ for (ϵ,δ)-differential privacy.

From Theorem 4.4, it is known that (4.2) is a sufficient condition of (ϵ,δ)-differential privacy. However, it should be pointed out that (4.2) is not a necessary condition of (ϵ,δ)-differential privacy (though it is a necessary condition of ϵ-differential privacy). An example is Gaussian noise, which is (ϵ,δ)-differentially private noise [3, 4], but (4.2) no longer holds for Gaussian noise. The detailed analysis will be given in the next subsection. Then, we give the other useful sufficient condition of (ϵ,δ)-differential privacy, which can be used to prove that adding Gaussian noise ensures (ϵ,δ)-differential privacy.

THEOREM 4.5. *Let $\Theta=\Theta_0\cup\Theta_1$. Assume that*

$$\oint_{\Theta_0} f_{\theta_i}(z)dz\le\delta,\forall i\in V \tag{4.16}$$

and (4.2) holds when $\theta\in\Theta_1$, i.e.,

$$\sup_{\hat{\sigma}\in[-\sigma,\sigma],\theta\in\Theta_1}\frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)}=c_b. \tag{4.17}$$

Then, $\mathcal{A}$ is (ϵ,δ)-differentially private, where $\epsilon=\log(c_b)$.

Proof. Given any σ-adjacent state vectors x and y satisfying $x_{i_0}=y_{i_0}-\sigma$ and $x_i=y_i$ (when $i\neq i_0$), we have

$$\begin{aligned}
&\Pr\{\mathcal{A}(x)\in\mathcal{O}\}=\prod_{l=1}^{n}\Pr\{\mathcal{A}(x_l)\in\mathcal{O}_l\}\\
&=\Pr\{\mathcal{A}(x_{i_0})\in\mathcal{O}_{i_0}\}\prod_{l=1,l\neq i_0}^{n}\Pr\{\mathcal{A}(x_l)\in\mathcal{O}_l\}\\
&\le[\Pr\{\mathcal{A}(x_{i_0})\in\mathcal{O}_{i_0}|\theta\in\Theta_0\}+\Pr\{\mathcal{A}(x_{i_0})\in\mathcal{O}_{i_0}|\theta\in\Theta_1\}]\\
&\quad\times\prod_{l=1,l\neq i_0}^{n}\Pr\{\mathcal{A}(y_l)\in\mathcal{O}_l\}\\
&\le c_b\Pr\{\mathcal{A}(y_{i_0})\in\mathcal{O}_{i_0}\}\prod_{l=1,l\neq i_0}^{n}\Pr\{\mathcal{A}(y_l)\in\mathcal{O}_l\}\\
&\quad+\oint_{\Theta_0}f_{\theta_i}(z)\mathrm{d}z\prod_{l=1,l\neq i_0}^{n}\Pr\{\mathcal{A}(y_l)\in\mathcal{O}_l\}\\
&\le c_b\Pr\{\mathcal{A}(y)\in\mathcal{O}\}+\delta.
\end{aligned}$$

Thus, we have completed the proof. □

Considering the conditions in Theorem 4.5, for any kinds of noise random distribution, we have

$$\lim_{\mu(\Theta_0)\to\mu(\Theta)} \oint_{\Theta_0} f_{\theta_i}(z)\mathrm{d}z = 1,$$

and

$$\lim_{\mu(\Theta_1)\to 0} \sup_{\hat{\sigma}\in[-\sigma,\sigma],\theta\in\Theta_1} \frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)} = 1.$$

Hence, it follows from Theorem 4.5 that using any kinds of random noise, $\mathcal{A}$ is $(0,1)$-differentially private. This can also shown from the fact that

$$\Pr\{\mathcal{A}(x)\in\mathcal{O}\} - \Pr\{\mathcal{A}(y)\in\mathcal{O}\} \le 1$$

holds for any kinds of noise adding mechanism (because $0 \le \Pr\{\cdot\} \le 1$ always holds true). Thus, it is meaningless to consider a $(0,1)$-differentially private mechanism, since it can be satisfied by any random distributions. Note that if $\Theta = \Theta_0(k)\cup\Theta_1(k)$ and $\Theta_0(k)\subset\Theta_0(k+1)$, where $\Theta_1(\infty)=\Theta$, then we have

$$\begin{aligned}\oint_{\Theta_0(k)} f_{\theta_i}(z)\mathrm{d}z &\le \oint_{\Theta_0(k+1)} f_{\theta_i}(z)\mathrm{d}z \\ &\le \oint_{\Theta_0(\infty)} f_{\theta_i}(z)\mathrm{d}z = 1\end{aligned}$$

while

$$\begin{aligned}\sup_{\hat{\sigma}\in[-\sigma,\sigma],\theta\in\Theta_1(k)} \frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)} &\ge \sup_{\hat{\sigma}\in[-\sigma,\sigma],\theta\in\Theta_1(k+1)} \frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)} \\ &\ge \sup_{\hat{\sigma}\in[-\sigma,\sigma],\theta\in\Theta_1(\infty)} \frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)} = 1,\end{aligned}$$

where we have used the fact that $\Theta_1(\infty)=\emptyset$. It means that there exists an increasing sequence $\delta(k)$ and an decreasing sequence $\epsilon(k)=\log(c(k))$ satisfying $\lim_{k\to\infty}\delta(k)=1$ and $\lim_{k\to\infty}\epsilon(k)=0$, respectively, such that $(\epsilon(k),\delta(k))$-differential privacy is guaranteed by $\mathcal{A}$. However, it should be pointed out that different noise distribution can guarantee the different smallest δ and different corresponding ϵ of (ϵ,δ)-differential privacy. In Theorem 4.4, the estimation of the upper bounds for δ and ϵ can be tighten for some special distributions (e.g., uniform distribution), which will be illustrated in the following subsection.

4.3. Case Studies. From the theoretical results obtained in above two subsections, it is not difficult to determine whether the added noise can guarantee the differential privacy of a random mechanism or not. In the following, we analyze differential privacy of some random noises.

First, for example 3.4, it is not obvious to analyze its differential privacy directly from the definition. But, from Theorem 4.2, we easily infer that it is not ϵ-differentially private, since $f_{\theta_i}(0)=0$, and thus it does not satisfy the necessary condition given in the theory.

Then, we consider the Laplacian noise adding mechanism. Assume that the PDF is $f_{\theta_i}(z)=\frac{1}{2b}e^{-\frac{|z-a|}{b}}$, where a and b are two constants. We check the conditions c_1

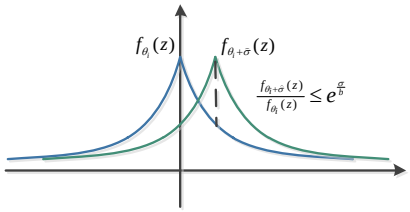

FIG. 4.2. *Laplacian noise: ϵ-differentially private.*

and c_2, respectively. From Fig. 4.2, it is clear that c_1 holds true due to the continuity and positivity of the PDF of Laplacian noise. Note that for $\forall \hat{\sigma} \in [-\sigma, \sigma]$, we have

$$\begin{aligned} |\frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)}| &= \frac{\frac{1}{2b}e^{-\frac{|z-\hat{\sigma}-a|}{b}}}{\frac{1}{2b}e^{-\frac{|z-a|}{b}}} \\ &= e^{\frac{|z-a|-|z-\hat{\sigma}-a|}{b}} \le e^{\frac{|\sigma|}{b}}. \end{aligned}$$

It means that c_2 condition also holds true. Hence, from Theorem 4.1, it follows that Laplacian noise is an ϵ-differentially private noise.

Next, we consider Gaussian noise. Assume that the PDF of the noise is $f_{\theta_i}(z) = \frac{1}{b\sqrt{2\pi}}e^{-\frac{(z-a)^2}{2b^2}}$. Similarly, one infers that c_1 holds true for Gaussian noise. Note that

$$\begin{aligned} |\frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)}| &= \frac{\frac{1}{b\sqrt{2\pi}}e^{-\frac{(z-\hat{\sigma}-a)^2}{2b^2}}}{\frac{1}{b\sqrt{2\pi}}e^{-\frac{(z-a)^2}{2b^2}}} = e^{\frac{(z-a)^2-(z-\hat{\sigma}-a)^2}{2b^2}} \\ &= e^{\frac{\hat{\sigma}(2z-\hat{\sigma}-2a)}{2b^2}}, \end{aligned}$$

which means that

$$\sup_{\hat{\sigma}\in[-\sigma,\sigma], f_{\theta_i}(z)\neq 0} \frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)} \ge \lim_{z\to\infty} e^{\frac{\hat{\sigma}(2z-\hat{\sigma}-2a)}{2b^2}} = \infty.$$

Hence, from Theorem 4.1, it follows that Gaussian noise is not an ϵ-differentially private noise. However, as shown in Fig. 4.3, there exists a large constant M such

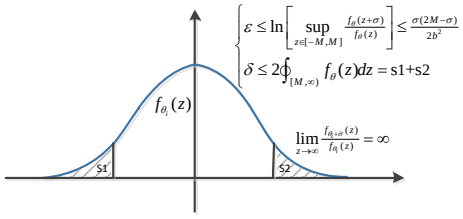

FIG. 4.3. *Gaussian noise: (ϵ, δ)-differentially private.*

that ϵ is bounded by

$$\epsilon \le \ln(\max e^{\frac{\hat{\sigma}(2z-\hat{\sigma}-2a)}{2b^2}}) \le \frac{\sigma(2M-\sigma)}{2b^2},$$

for $z \in [-M, M]$, and δ is bounded by

$$\begin{aligned}\delta &\leq \oint_{(-\infty,-M]\cup[M,\infty)} f_{\theta_i}(z)\mathrm{d}z \\ &= \frac{1}{b\sqrt{2\pi}} \oint_{(-\infty,-M]\cup[M,\infty)} e^{-\frac{(z-a)^2}{2b^2}}\mathrm{d}z,\end{aligned}$$

which is a small value. It means that the conditions in Theorem 4.5 can be satisfied. Thus, we infer that Gaussian noise is an (ϵ, δ)-differentially private noise.

Lastly, consider the uniform distribution noise with its PDF as $\frac{1}{b-a}$. Clearly, c_1 is not true due to the infinite measure of the zero-point set. Hence, uniform distribution is not an ϵ-differentially private noise. Then, we check the conditions in Theorem 4.4. As shown in Fig. 4.4, it is found that for an uniform distribution noise

$$\sup_{\hat{\sigma}\in[-\sigma,\sigma], f_{\theta_i}(z)\neq 0} \frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)} = \frac{\frac{1}{b-a}}{\frac{1}{b-a}} = 1$$

and

$$\max_{i\in V} \oint_{\Phi_i^0} f_{\theta_i}(z+\sigma)\mathrm{d}z = \frac{\sigma}{b-a}.$$

It means that the upper bounds of both ϵ and δ in Theorem 4.4 are tight. Thus, one infers that uniform noise is an (ϵ, δ)-differentially private noise, where $\epsilon = 0$ and $\delta = \frac{\sigma}{b-a}$. Then, it is noted that δ is a decreasing function of $b-a$ and satisfies

$$\lim_{b-a\to\infty} \delta = 0.$$

Hence, for any small δ, we can find a corresponding $(0, \delta)$-differentially private uniform noise. But, it should be pointed out that when the value of $b-a$ increases, the variance of the uniform distribution $(= \frac{(b-a)^2}{12})$ increases.

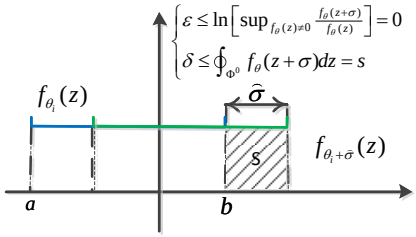

FIG. 4.4. *Uniform noise:* $(0, \delta)$*-differentially private.*

The above analysis shows that our method can determine the differential privacy of the randomized mechanism with any given distribution of noise by checking the conditions, and thus it is an efficient criterion of differential privacy analysis. Also, using our theory, we can obtain the same results for well-known noise distributions, as those proved in the existing work, which verifies the effectiveness of the proposed theory.

5. Application on privacy-preserving consensus algorithm. Consensus algorithm is an efficient distributed computing and control algorithm, which refers to the action that nodes in the network reach a global agreement regarding a certain opinion using their local neighbors' information only [14–16]. Consensus algorithm has been applied in a variety of areas, e.g., distributed energy management [17], scheduling [18], and clock synchronization [19–21]. Recently, the privacy-preserving consensus problem has been studied, which aims to guarantee that the privacy of initial state is preserved and at the same time a consensus can still be achieved [22, 26, 28]. The basic idea is to add random noises to the real state value during the communication for privacy preservation, the same as (3.3). This motivates us to adopt the developed theories in the above section to analyze differential privacy of the privacy-preserving consensus algorithm.

5.1. Privacy-preserving Consensus Algorithm. A network is abstracted by an undirected and connected graph, $G = (V, E)$, where V is the set of nodes and E is the set of the communication links (edges) between nodes. An edge $(i, j) \in E$ iff nodes i and j can communicate with each other. Let N_i be the neighbor set of node i, defined by $N_i = \{j | j \in V, (i, j) \in E, j \neq i\}$. Let $|V| = n \geq 3$ be the number of nodes in the network and $x_i(0) \in \mathbf{R}$ be the initial state of node i. Let $x(0) = [x_1(0), ..., x_n(0)]^T \in \Omega_x^0 \subseteq \mathbf{R}^n$.

General Consensus Algorithm: For a general consensus algorithm, each node will communicate with its neighbor nodes and update its state based on the received information. The dynamic iteration equation is given by

$$x_i(k+1) = w_{ii}x_i(k) + \sum_{j \in N_i} w_{ij}x_j(k), \forall i \in V, \tag{5.1}$$

which can be written in the matrix form as

$$x(k+1) = Wx(k), \tag{5.2}$$

where w_{ii} and w_{ij} are weights, and W is the weight matrix. It is well known from [31] that, if, i) $w_{ii} > 0$ and $w_{ij} > 0$; and ii) W is a doubly stochastic matrix, then an average consensus can be achieved by (5.2), i.e.,

$$\lim_{k \to \infty} x(k) = \frac{\sum_{\ell=1}^{n} x_\ell(0)}{n} \mathbf{1} = \bar{x}. \tag{5.3}$$

Privacy-preserving Consensus (PC) Algorithm: When the privacy of nodes' initial states are concerned, each node may be unwilling to release its real state to the neighbor nodes at each iteration. To preserve the privacy of nodes' initial states, a widely used approach is to add a random noise to the real state when a node needs to communicate with its neighbor nodes [28]. Hence, we introduce a common privacy-preserving consensus algorithm as follows:

$$\mathcal{PC}: \begin{cases} x^+(k) = x(k) + \theta(k) \\ x(k+1) = Wx^+(k) \end{cases} \tag{5.4}$$

A privacy-preserving average consensus algorithm is to design the adding noise process (including the noise distribution and the correlations among noises in different iterations), such that the goal of (5.3) is achieved under (5.4).

5.2. Privacy Conditions of Consensus. We define the input and the output sequences of each node i in privacy-preserving consensus algorithm (5.4) until iteration k as

$$\mathcal{I}_{x_i}^{in}(k) = \{x_i(0), \theta_i(0), ..., \theta_i(k)\}, \tag{5.5}$$

and

$$\mathcal{I}_{x_i}^{out}(k) = \{x_i^+(0), ..., x_i^+(k)\}, \tag{5.6}$$

respectively. Then, $\mathcal{I}_x^{in}(k) = \{x(0), \theta(0), ..., \theta(k)\}$ is the system input and $\mathcal{I}_x^{out}(k) = \{x^+(0), ..., x^+(k)\}$ is the system output. Let the information set of the adding noises for node i be $\mathcal{I}_{i_{noise}}^{in}(k) = \{\theta_i(0), ..., \theta_i(k)\}$. Let $f_{\theta_i(k)}(z)$ be the PDF of $\theta_i(k)$. Then, we have Range$(\mathcal{PC}) = \Omega_x^0 \oplus \Theta(0) \oplus ... \oplus \Theta(k) \oplus ...$, where $\oplus$ denotes the plus of two sets.

By referring to [26], we introduce the definition of (ϵ, δ)-differential privacy for a consensus algorithm as follows.

DEFINITION 5.1. *A PC algorithm (5.4) is (ϵ, δ)-differentially private if, for any pair x and y of σ-adjacent initial state vector and any set $\mathcal{O} \subseteq \mathbf{R}^{n\times\infty}$,*

$$\Pr\{\mathcal{I}_x^{out}(\infty) \in \mathcal{O}\} \leq e^{\epsilon} \Pr\{\mathcal{I}_y^{out}(\infty) \in \mathcal{O}\} + \delta. \tag{5.7}$$

If $\delta = 0$, we say that (5.4) is ϵ-differentially private.

First, we give the necessary condition of ϵ-differential privacy for algorithm (5.4).

THEOREM 5.2. *If algorithm (5.4) is ϵ-differentially private, then $\forall k \geq 0$, the random noise vector $\sum_{l=0}^{k} W^{k-l}\theta(l)$ should satisfy conditions c_1 and c_2.*

Proof. Let $\mathcal{O}^{n\times k} \subseteq \mathbf{R}^{n\times \mathbf{k}}$ for $k > 0$ and $\mathcal{O}^{n\times 0} \subseteq \mathbf{R}^n$ for $k = 0$. For any pair x and y of σ-adjacent initial state vectors, we have

$$\begin{aligned}
&\Pr\{\mathcal{I}_x^{out}(\infty) \in \mathcal{O}\} \leq e^{\epsilon} \Pr\{\mathcal{I}_y^{out}(\infty) \in \mathcal{O}\}, \forall \mathcal{O} \subseteq \mathbf{R}^{n\times\infty} \\
\Leftrightarrow &\Pr\{\mathcal{I}_x^{out}(k) \in \mathcal{O}^{n\times k}\} \leq e^{\epsilon} \Pr\{\mathcal{I}_y^{out}(k) \in \mathcal{O}^{n\times k}\}, \qquad (5.8)\\
&\forall k \geq 0, \mathcal{O}^{n\times k} \subseteq \mathbf{R}^{n\times k} \\
\Rightarrow &\Pr\{x^+(k) \in \mathcal{O}^{n\times 1}\} \leq e^{\epsilon} \Pr\{y^+(k) \in \mathcal{O}^{n\times 1}\}, \qquad (5.9)\\
&\forall k \geq 0, \mathcal{O}^{n\times k} \subseteq \mathbf{R}^{n\times k}.
\end{aligned}$$

From (5.4), we have

$$\begin{aligned}
x^+(k) &= x(k) + \theta(k) \\
&= W[x(k-1) + \theta(k-1)] + \theta(k) \\
&= W^k x(0) + \sum_{l=0}^{k} W^{k-l}\theta(l) \\
&= x(0) + (W^k - I)x(0) + \sum_{l=0}^{k} W^{k-l}\theta(l), \qquad (5.10)
\end{aligned}$$

where I is an identity matrix. From (5.8), (5.10) and Theorem 4.1, we infer that $(W^k - I)z + \sum_{l=0}^{k} W^{k-l}\theta(l), z = x, y$ should satisfy conditions c_1 and c_2 for any σ-adjacent state vectors x and y. It follows that $\sum_{l=0}^{k} W^{k-l}\theta(l)$ satisfies conditions c_1 and c_2. □

Then, the sufficient conditions of differential privacy for algorithm (5.4) is obtained in the following theorem.

THEOREM 5.3. *Suppose that the noise sequence $\theta(1), \theta(2), ..., \theta(k), ...,$ is independent from both $\theta(0)$ and $x(0)$. Then, if $\theta(0)$ satisfies conditions c_1 and c_2, algorithm (5.4) provides ϵ-differential privacy; if $\theta(0)$ satisfies (4.2) or (both (4.16) and (4.17) simultaneously), algorithm (5.4) provides (ϵ, δ)-differential privacy, where $\epsilon = \log(c_b)$ and δ satisfies (4.15) or (4.16).*

Proof. Given any $\mathcal{O} \subseteq \mathbf{R}^{n\times\infty}$, we let $\mathcal{O}_l^\iota$ be the set of the l-th to ι-th column vectors of $\mathcal{O}$ for $l, \iota \in \mathbf{N}^+$. Then,

$$\begin{aligned}
&\Pr\{\mathcal{I}_x^{out}(\infty) \in \mathcal{O}\} \\
=&\Pr\{x^+(0) \in \mathcal{O}_1^1\} \Pr\{\mathcal{I}_x^{out}(1,\infty) \in \mathcal{O}_2^\infty | x^+(0) \in \mathcal{O}_1^1\} \\
=&\oint_{\mathcal{O}_1^1} f_{\theta(0)}(z-x) \Pr\{\mathcal{I}_x^{out}(1,\infty) \in \mathcal{O}_2^\infty | z\} \mathrm{d}z
\end{aligned}$$

and

$$\begin{aligned}
&\Pr\{\mathcal{I}_y^{out}(\infty) \in \mathcal{O}\} \\
=&\Pr\{y^+(0) \in \mathcal{O}_1^1\} \Pr\{\mathcal{I}_y^{out}(1,\infty) \in \mathcal{O}_2^\infty | y^+(0) \in \mathcal{O}_1^1\} \\
=&\oint_{\mathcal{O}_1^1} f_{\theta(0)}(z-y) \Pr\{\mathcal{I}_y^{out}(1,\infty) \in \mathcal{O}_2^\infty | z\} \mathrm{d}z
\end{aligned}$$

Since $\theta(1), \theta(2), ..., \theta(k), ...,$ are independent from both $\theta(0)$ and $x(0)$, for any given same vector z, we have

$$\Pr\{\mathcal{I}_x^{out}(1,\infty) \in \mathcal{O}_2^\infty | z\} = \Pr\{\mathcal{I}_y^{out}(1,\infty) \in \mathcal{O}_2^\infty | z\}.$$

When $\theta(0)$ satisfies conditions c_1 and c_2, we have

$$\begin{aligned}
&\oint_{\mathcal{O}_1^1} f_{\theta(0)}(z-x) \Pr\{\mathcal{I}_x^{out}(1,\infty) \in \mathcal{O}_2^\infty | z\} \mathrm{d}z \\
=&\oint_{\mathcal{O}_1^1} f_{\theta(0)}(z-y+\sigma) \Pr\{\mathcal{I}_x^{out}(1,\infty) \in \mathcal{O}_2^\infty | z\} \mathrm{d}z \\
=&\oint_{\mathcal{O}_1^1} f_{\theta_{i_0}(0)}(z_{i_0}-y_{i_0}+\sigma_{i_0}) \prod_{i=1, i\neq i_0}^{n} f_{\theta_i(0)}(z_i-y_i) \\
&\times \Pr\{\mathcal{I}_x^{out}(1,\infty) \in \mathcal{O}_2^\infty | z\} \mathrm{d}z \\
\leq&\oint_{\mathcal{O}_1^1} c_b f_{\theta(0)}(z-y) \Pr\{\mathcal{I}_y^{out}(1,\infty) \in \mathcal{O}_2^\infty | z\} \mathrm{d}z,
\end{aligned}$$

where $\sigma \in \mathbf{R}^n$ is a vector with $\sigma_{i_o} = \sigma$ and all the other elements equal to 0, which means that

$$\Pr\{\mathcal{I}_x^{out}(\infty) \in \mathcal{O}\} \leq e^\epsilon \Pr\{\mathcal{I}_y^{out}(\infty) \in \mathcal{O}\}.$$

Thus, (5.4) provides ϵ-differential privacy.

When $\theta(0)$ satisfies (4.2), we have

$$\begin{aligned}
&\oint_{\mathcal{O}_1^1} f_{\theta(0)}(z-x)\Pr\{\mathcal{I}_x^{out}(1,\infty)\in\mathcal{O}_2^\infty|z\}\mathrm{d}z\\
\le&\oint_{\mathcal{O}_1^1} c_b f_{\theta(0)}(z-y)\Pr\{\mathcal{I}_y^{out}(1,\infty)\in\mathcal{O}_2^\infty|z\}\mathrm{d}z\\
&+\oint_{\hat{\mathcal{O}}_1^1} f_{\theta(0)}(z-x)\Pr\{\mathcal{I}_y^{out}(1,\infty)\in\mathcal{O}_2^\infty|z\}\mathrm{d}z\\
\le&\oint_{\mathcal{O}_1^1} c_b f_{\theta(0)}(z-y)\Pr\{\mathcal{I}_y^{out}(1,\infty)\in\mathcal{O}_2^\infty|z\}\mathrm{d}z\\
&+\oint_{\hat{\mathcal{O}}_1^1} f_{\theta(0)}(z-x)\mathrm{d}z
\end{aligned}$$

where $\hat{\mathcal{O}}_1^1=\{z|z\in\mathcal{O}_1^1, f_{\theta_{i_0}(0)}(z_{i_0}-y_{i_0})=0, f_{\theta_{i_0}(0)}(z_{i_0}-x_{i_0})\neq 0\}$. Let δ satisfy (4.15). Then, we have

$$\Pr\{\mathcal{I}_x^{out}(\infty)\in\mathcal{O}\}\le e^\epsilon\Pr\{\mathcal{I}_y^{out}(\infty)\in\mathcal{O}\}+\delta.$$

Thus, (5.4) provides (ϵ,δ)-differential privacy.

If $\theta(0)$ satisfies both (4.16) and (4.17) simultaneously, then there also exists Θ_0 and Θ_1 such that $\theta(0)+x$ satisfies (4.16) and (4.17). Hence, we have

$$\begin{aligned}
&\Pr\{\mathcal{I}_x^{out}(\infty)\in\mathcal{O}\}\\
=&\oint_{\mathcal{O}_1^1} f_{\theta(0)}(z-x)\Pr\{\mathcal{I}_x^{out}(1,\infty)\in\mathcal{O}_2^\infty|z\}\mathrm{d}z\\
=&\oint_{\mathcal{O}_1^1\cap\Theta_0} f_{\theta(0)}(z-x)\Pr\{\mathcal{I}_x^{out}(1,\infty)\in\mathcal{O}_2^\infty|z\}\mathrm{d}z\\
&+\oint_{\mathcal{O}_1^1\cap\Theta_1} f_{\theta(0)}(z-x)\Pr\{\mathcal{I}_x^{out}(1,\infty)\in\mathcal{O}_2^\infty|z\}\mathrm{d}z\\
\le&\oint_{\Theta_0} f_{\theta(0)}(z-x)\mathrm{d}z\\
&+c_b\oint_{\mathcal{O}_1^1\cap\Theta_1} f_{\theta(0)}(z-y)\Pr\{\mathcal{I}_y^{out}(1,\infty)\in\mathcal{O}_2^\infty|z\}\mathrm{d}z\\
\le&\delta+\log(c_b)\Pr\{\mathcal{I}_y^{out}(\infty)\in\mathcal{O}\}.
\end{aligned}$$

It means that (5.4) provides (ϵ,δ)-differential privacy.

Thus, we have completed the proof. □

5.3. Privacy Analysis of PC Algorithms. We first give the necessary condition of average consensus for algorithm (5.4).

THEOREM 5.4. *Using algorithm (5.4), if*

$$\Pr\{\lim_{k\to\infty}x(k)=\bar{x}\}=1, \tag{5.11}$$

i.e., the average consensus is achieved almost surely, then

$$\Pr\{\lim_{k\to\infty}\sum_{l=0}^{k-1}W^{k-l}\theta(l)=0\}=1,$$

and $\Pr\{\lim_{k\to\infty} W\theta(k) = 0\} = 1$*, i.e., the added noise should equal* 0 *or be the eigenvector of* 0 *when* $k \to \infty$*.*

Proof. Under algorithm (5.4), we have

$$\begin{aligned}\lim_{k\to\infty} x(k) &= \lim_{k\to\infty}\left[W^k x(0) + \sum_{l=0}^{k-1} W^{k-l}\theta(l)\right] \\ &= \lim_{k\to\infty} W^k x(0) + \lim_{k\to\infty}\sum_{l=0}^{k-1} W^{k-l}\theta(l) \\ &= \bar{x} + \lim_{k\to\infty}\sum_{l=0}^{k-1} W^{k-l}\theta(l),\end{aligned}$$

where set $\sum_{l=1}^{-1}(\cdot) = 0$. Then, from (5.11), it follows that

$$\begin{aligned}\Pr\{\lim_{k\to\infty}\sum_{l=0}^{k-1} W^{k-l}\theta(l) = 0\} &= \Pr\{\lim_{k\to\infty}[x(k) - \bar{x}] = 0\} \\ &= 1.\end{aligned}$$

Then, note that when $\sum_{l=0}^{k-1} W^{k-l}\theta(l) = 0$, we have $W\theta(\infty) = 0$. Hence, we have $\Pr\{\lim_{k\to\infty} W\theta(k) = 0\} = 1$. □

Next, by comparing the necessary conditions of ϵ-differential privacy and average consensus, an impossibility result is given as follows.

Impossibility Result: From Theorem 5.4, one infers that the added noise $\theta(k)$ should converge to 0 or the 0-eigenvector of W, denoted by λ_0, i.e., $\lim_{k\to\infty}\theta(k) = 0$ or $\lim_{k\to\infty}\theta(k) = \lambda_0$. Note that

$$\lim_{k\to\infty}\sum_{l=0}^{k} W^{k-l}\theta(l) = \lim_{k\to\infty}\left[\sum_{l=0}^{k-1} W^{k-l}\theta(l) + \theta(k)\right].$$

Then, we have

$$\Pr\{\lim_{k\to\infty}\sum_{l=0}^{k} W^{k-l}\theta(l) = 0 \text{ or } \lambda_0\} = 1.$$

Thus, the conditions c_1 and c_2 no longer hold for the added noise $\sum_{l=0}^{k} W^{k-l}\theta(l)$ when $k \to \infty$. It contradicts with the necessary condition in Theorem 5.2, and thus ϵ-differential privacy cannot be guaranteed. It means that the necessary condition of differential privacy and the necessary condition of average consensus are conflicted, which leads to the impossibility result. Hence, using (5.4), nodes cannot simultaneously converge to the average of their initial states and preserve ϵ-differential privacy of their initial states.

Also, it is not difficult to analyze differential privacy of the existing privacy-preserving consensus algorithm. For example, in [24, 26], the privacy-preserving consensus algorithms are designed by adding independent and Laplacian noise to the consensus process, and thus the sufficient conditions in Theorem 5.3 are satisfied. Hence, these privacy-preserving consensus algorithms proposed in [24, 26] are ϵ-differentially private, while the exact average consensus cannot be guaranteed by these algorithms.

In [28], the exponentially decaying and zero-sum normal noises are adopted in the privacy-preserving consensus algorithm. Since the sum of all added noises equals 0, the necessary condition in Theorem 5.2 cannot be satisfied. Hence, the algorithm proposed in [28] is not ϵ-differentially private. The authors used the disclosed subspace to quantify the privacy, and proved that with the proposed algorithm, the disclosed space of an agent with m neighbors is of dimension $m+1$. That is, as long as an agent cannot listen to agent i and all its essential neighbors, it cannot estimate the initial condition $x_i(0)$ perfectly.

6. Conclusions. In this paper, we provided different conditions of differential privacy for a generally random noise mechanism. We obtained the conditions for determining differential privacy of random noise mechanism, followed by an application study on privacy-preserving consensus algorithm. Specifically, considering a generally random noise adding mechanism, we obtained a necessary and sufficient condition of ϵ-differential privacy, and two useful sufficient conditions of (ϵ, δ)-differential privacy of the noise adding mechanism. We also provided the estimations of the upper bounds of the parameters ϵ and δ. Then, we showed that the obtained theory provides efficient and simple criteria of differential privacy using case studies. In addition, we applied the obtained result to obtain the necessary condition and the sufficient condition for the privacy-preserving consensus algorithm, under which differential privacy is achieved.

There are still many open issues worth further investigation. For example, in this paper, we focus on the privacy analysis, and do not consider the accuracy of queries from statistical databases under the random noise adding mechanism. How the distribution of the adding noise affect the accuracy of queries needs further investigation. Meanwhile, the relationship between the parameters in differential privacy (ϵ and δ), the parameters of the PDF of the adding noise (mean and variance) also needs further investigation.

REFERENCES

[1] J. He and L. Cai, "Differential private noise adding mechanism: basic conditions and its applicationin," *Proc. of IEEE ACC*, 2017.

[2] C. Dwork, "Differential privacy," in *Automata, languages and programming*, Springer, 1-12, 2006.

[3] Q. Geng and P. Viswanath, "The optimal noise-adding mechanism in differential privacy," *IEEE Transactions on Information Theory*, 62(2): 925-951, 2016.

[4] C. Dwork, "Differential privacy: A survey of results," in *Theory and Applications of Models of Computation, ser. Lecture Notes in Computer Science, M. Agrawal, D. Du, Z. Duan, and A. Li, Eds.* Springer Berlin Heidelberg, 1–19, 2008.

[5] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Foundations and Trends in Theoretical Computer Science*, 9(3-4), 211-407, 2014.

[6] J. Cortes, G. Dullerud, S. Han, J. Le Ny, S. Mitra, and G. J. Pappas. Differential privacy in control and network systems.*Proc. of IEEE CDC*, 2016.

[7] J. Hsu, A. Roth, T. Roughgarden, and J. Ullman, "Privately solving linear programs," in *Automata, Languages, and Programming*, ser. Lecture Notes in Computer Science, J. Esparza, P. Fraigniaud, T. Husfeldt, and E. Koutsoupias, Eds. Springer Berlin Heidelberg, 2014.

[8] S. Han, U. Topcu, and G. Pappas, "Differentially private convex optimization with piecewise affine objectives," in *Proc. of IEEE CDC*, 2014.

[9] M. Abadi, A. Chu, I. Goodfellow, H. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep Learning with differential privacy," *arXiv preprint arXiv:1607.00133*, 2016.

[10] G. Barthe, M. Gaboardi, B. Gregoire, J. Hsu, and P. Strub, "Advanced probabilistic couplings for differential privacy," *arXiv preprint arXiv:1606.07143*, 2016.

[11] F. McSherry, and Talwar, "Mechanism design via differential privacy," in *Proc. IEEE FOCS*, 2007.

[12] Q. Geng, P. Kairouz, S. Oh, and P. Viswanath. "The staircase mechanism in differential privacy," *IEEE Journal of Selected Topics in Signal Processing*, 9(7): 1176-1184, 2015.

[13] R. Hall, A. Rinaldo, and L. Wasserman,"Differential privacy for functions and functional data," *Journal of Machine Learning Research*, 14(2): 703-727, 2013.

[14] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proceedings of the IEEE*, 95(1): 215–233, 2007.

[15] A. Olshevsky and J. Tsitsiklis, "Convergence speed in distributed consensus and averaging," *SIAM Journal on Control and Optimization*, 48(1), 33–55, 2009.

[16] I. Matei, J. Baras, and C. Somarakis, "Convergence results for the linear consensus problem under markovian random graphs," *SIAM Journal on Control and Optimization*, 51(2), 1574–1591, 2013.

[17] C. Zhao, J. He, P. Cheng and J. Chen, "Consensus-based energy management in smart grid with transmission losses and directed communication," *IEEE Trans. on Smart Grid*, DOI: 10.1109/TSG.2015.2513772, 2015.

[18] J. He, L. Duan, F. Hou, P. Cheng, and J. Chen, "Multi-period scheduling for wireless sensor networks: A distributed consensus approach," *IEEE Trans. on Signal Processing*, 63(7): 1651-1663, 2015.

[19] L. Schenato and F. Fiorentin, "Average timesynch: A consensus-based protocol for clock synchronization in wireless sensor networks," *Automatica*, 47(9): 1878–1886, 2011.

[20] R. Carli, and S. Zampieri, "Network clock synchronization based on the second order linear consensus algorithm," *IEEE Trans Automat. Contr.*, 59(2): 409–422, 2014.

[21] J. He, P. Cheng, L. Shi, and J. Chen, "Time synchronization in WSNs: A maximum value based consensus approach," *IEEE Trans Automat. Contr.*, 59(3): 660–674, 2014.

[22] J. Le Ny and G. Pappas, "Differentially private filtering," *IEEE Trans Automat. Contr.*, 59(2): 341–354, 2014.

[23] S. Han, U. Topcu, and G. Pappas, " Differentially private distributed constrained optimization." *IEEE Transactions on Automatic Control*, 62(1), 50-64, 2017.

[24] Z. Huang, S. Mitra, and G. Dullerud, "Differentially private iterative synchronous consensus." in *Proc. ACM workshop on Privacy in the electronic society*, 2012.

[25] Z. Huang, S. Mitra, and N. Vaidya, "Differentially private distributed optimization. in *Proc. ACM ICDCN*, 2015.

[26] E. Nozari, P. Tallapragada, and J. Cortes, "Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design." *Automatica*, 81, 221-231, 2017.

[27] N. Manitara and C. Hadjicostis, "Privacy-preserving asymptotic average consensus." in *Proc. IEEE ECC*, 2013.

[28] Y. Mo, and R. Murray, "Privacy preserving average consensus," *IEEE Trans Automat Contr.*, 62(2): 753–765, 2017.

[29] M. DeGroot, "Reaching a consensus," *Journal of the American Statistical Association*, 69(345), 118–121, 1974.

[30] L. Wasserman and S. Zhou. A statistical framework for differential privacy. *Journal of the American Statistical Association*, 105(489), 375-389, 2010.

[31] A. Olshevsky and J. Tsitsiklis, "Convergence speed in distributed consensus and averaging," *SIAM Review*, 53(4): 747–772, 2011.

[32] W. Wang, L. Ying, and J. Zhang, "On the relation between identifiability, differential privacy, and mutual-information privacy," *IEEE Transactions on Information Theory*, to appear, 2017.

[33] K. Nissim, S. Raskhodnikova, and A. Smith. "Smooth sensitivity and sampling in private data analysis." in *Proc. ACM Symposium on Theory of Computing*, 2007.