Differential Private Noise Adding Mechanism and Its Application on Consensus Algorithm*

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 (single-dimensional case) 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 not only matches with the literature, but also provides an efficient approach to the privacy parameters' estimation; 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.**

***Index Terms*—Random mechanism, Noise adding process, Average consensus, Differential privacy**

I. 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 control and signal processing 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 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 privacy parameters 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

* Part of the preliminary result of this work was presented by IEEE Conference on American Control Conference (ACC), 2017 [1].

†: The Dept. of Automation, Shanghai Jiao Tong University, and the Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai, China jianpinghe.zju@gmail.com, jphe@sjtu.edu.cn, xpguan@sjtu.edu.cn

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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSP.2020.3006760, IEEE Transactions on Signal Processing

the obtained results, it is easy to obtain the properties of differential privacy for any adding noise, even when the probability density function is unknown.

- 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. Section II formulates the problem. In Section III, we provide the basic theoretical results of differential privacy. Section IV studies the application on privacy-preserving consensus algorithm. The related works are given in Section V. Conclusions are summarized in Section VI.

II. Preliminary and Problem Formulation

A. Preliminary

Let $V = \{1, 2, ..., n\}$ be the set of nodes (users). Following [25]–[28], we define σ-adjacency and differential privacy, respectively, as follows.

Definition 2.1 (σ-adjacency): Given $\sigma \in \mathbf{R}^+$, the state vector x and y are σ-adjacent if, for some $i_0 \in V$,

$$|x_i - y_i| \leq \begin{cases} \sigma, & \text{if } i = i_0; \\ 0, & \text{if } i \neq i_0, \end{cases} \tag{1}$$

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. It should be pointed out that in the standard setting of multi-dimensional differential privacy, global sensitivity is defined using L_1 or L_2 norm. This paper uses σ-adjacency to characterize the sensitivity, under which the multi-dimensional problem can be reduced to a single-dimensional case, which makes the problem much easier to solve. Thus, the resulting theoretical conclusion of conditions on differential privacy can be of an explicit form, and can further facilitate future research on more general cases.

Definition 2.2 ((ϵ, δ)-differential privacy): A randomized mechanism $\mathcal{A}$ with domain Ω is (ϵ, δ)-differentially private if, for any pair x and y ($x, y \in \Omega \subseteq \mathbf{R}^n$) of σ-adjacent state vector and any set $\mathcal{O} \subseteq \text{Ra}(\mathcal{A})$, where $\text{Ra}(\mathcal{A})$ is the domain of the output under mechanism $\mathcal{A}$,

$$\Pr\{\mathcal{A}(x) \in \mathcal{O}\} \leq e^{\epsilon} \Pr\{\mathcal{A}(y) \in \mathcal{O}\} + \delta. \tag{2}$$

If $\delta = 0$, we say that $\mathcal{A}$ is ϵ-differentially private.

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. Typically, the values of δ should be less than the inverse of any polynomial in the size of the database [5]. ϵ-differentially private usually provides a stronger privacy than (ϵ, δ)-differential privacy. Compare with the original definition of differential privacy given in [2], the above definition can also be used to the continuous and infinite dimensional data.

TABLE I
Notations

Symbol	Definition
x, y	a pair of σ-adjacent n dimensional vector
$\mathcal{A}$	a random mechanism
$\oint$	an integral where the variable can be in discontinuous intervals
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 $\text{Ra}(\mathcal{A})$
$\mathcal{O}_i$	the set of i-th column element of $\mathcal{O}$
$\text{Ra}(\mathcal{A})$	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

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

B. Problem Formulation

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

$$\mathcal{A}(x) = x + \theta, \ \forall \ x \in \Omega, \tag{3}$$

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 $\Theta \subseteq R^n$. Then, we have $\text{Ra}(\mathcal{A}) = \Omega \oplus \Theta$, where $\oplus$ denotes the Minkowski sum between two set, i.e., any element in $\text{Ra}(\mathcal{A})$ will equal to the sum of two elements in sets Ω and Θ. In this paper, we consider the case that Ω is not a discrete set and $f_{\theta_i}(z)$ is not a probability mass function. Thus, we have the following three basic assumptions:

- A_1: the set of all possible values of nodes' state at least contains an almost surely continuous interval.
- A_2: each $f_{\theta_i}(z)$ is an almost surely continuous or piecewise continuous function.
- A_3: θ_i and θ_j are independent from each other for $\forall i \neq j$ (nodes can add noises independently in applications).

The random mechanism $\mathcal{A}$ defined in (3) is a general continuous 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]. Thus,

[1]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.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSP.2020.3006760, IEEE Transactions on Signal Processing

most of the existing random mechanisms can be mathematically modeled to this noise adding process, e.g., widely used Laplacian noise adding mechanism [5], [28].

When the noises' probability density functions (PDF) are well known functions, e.g., Laplacian and Gaussian, it is not difficult to prove that, whether they are ϵ-differential privacy or not, using the definition of the differential privacy. This is mainly because that these functions have well properties, e.g., easy to calculation. However, when the PDF becomes more complicate or even cannot be expressed in a closed form. It is hard to prove it. Considering the following examples.

Example 2.3: The PDF of the noise in (3) follows

$$f_{\theta_i}(z) = \begin{cases} \frac{z}{2}e^{-z}, & z \geq 0; \\ \frac{-z}{2}e^{z}, & z \leq 0, \end{cases} \tag{4}$$

Example 2.4: The PDF of the noise in (3) satisfies $f_{\theta_i}(z) = \sum_{k=1}^{m} \nu_k f_k(z)$, where ν_k is the weight and each $f_k(z)$ follows an Gaussian distribution. Clearly, $f_{\theta_i}(z)$ is a mixed Gaussian distribution function.

It is not easy to determine or prove that whether $\mathcal{A}$ achieves ϵ-differential privacy or not. Furthermore, how to make a good estimation of the values of ϵ and δ is also an interesting and challenging problem.

Problem of Interests: Motivated by the above analysis, therefore, the goal of this paper is to investigate the following issues: i) What are general properties of differential privacy considering (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 $\mathcal{A}$. And, how to estimate the values of the corresponding privacy parameters, i.e., ϵ and δ, when the noise' distribution is given. ii) Can we find a noise distribution such that $\mathcal{A}$ is ϵ-differentially private for any small ϵ. iii) How to extend and apply the obtained results for privacy analysis on the privacy-preserving consensus algorithm, an important distributed iterative algorithm in the cooperative control area. We solve these problems in the following two sections.

III. Conditions of Differential Privacy

In this section, the basic conditions of differential privacy considering $\mathcal{A}$ defined in (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 $\{\cdot\} \neq 0$.

A. 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 3.1: $\mathcal{A}$ is ϵ-differentially private if and only if (iff) the following two conditions hold,

c_1: let $\Phi_i^0 = \{z | f_{\theta_i}(z) = 0, z \in \mathbf{R}\}$, then for $\forall i \in V$, there $\nexists$ a continuous interval $[a, b]$ such that

$$[a, b] \subseteq \Phi_i^0, \tag{5}$$

where $a, b \in \mathbf{R}$ and $b > a$;

c_2: there $\exists$ a positive constant c_b such that

$$\sup_{\hat{\sigma} \in [-\sigma, \sigma], f_{\theta_i}(z) \neq 0, i \in V} \frac{f_{\theta_i + \hat{\sigma}}(z)}{f_{\theta_i}(z)} = c_b, \tag{6}$$

where $\epsilon = \log(c_b)$, and 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. Meanwhile, since c_b is a supremum satisfying (6), it is a constant when the distribution functions and parameter σ are given. On the other hand, when σ becomes larger, it is not difficult to infer that c_b becomes larger, so the value of c_b is an increasing function of σ. In addition, 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 3.1 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. Thus, c_2' can be applied to determine whether c_2 is true or not.

Remark 3.2: In the above Theorem 3.1, c_1 ensures that any pair of the adjacency vectors cannot have totally different outputs in the probability sense. Hence, the privacy attacker cannot determine whether an element in the input or not from the observed outputs, thus the differential privacy is ensured. c_2 decides the values of ϵ and ensures that ϵ is a bounded constant and will not go to infinity at any point.

Based on Theorem 3.1, users can directly verify whether the mechanism is differentially private or not through verifying the property of noise distribution function. It is different from the existing work (e.g., [3], [5]), focusing on specific mechanisms (e.g., Laplace mechanism and Exponential mechanism), where the privacy was proved from the original definition of ϵ-differential privacy.

It is well known that a smaller ϵ provides a stronger privacy guarantee. 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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSP.2020.3006760, IEEE Transactions on Signal Processing

satisfied. The PDF is

$$f(z)=\begin{cases}\dfrac{1-\varrho}{2a}\varrho^k, & z\in[ka,(k+1)a];\\ \dfrac{1-\varrho}{2a}, & z\in[-a,a];\\ \dfrac{1-\varrho}{2a}\varrho^k, & z\in[-ka-a,-ka],\end{cases}\tag{7}$$

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. 1. For the

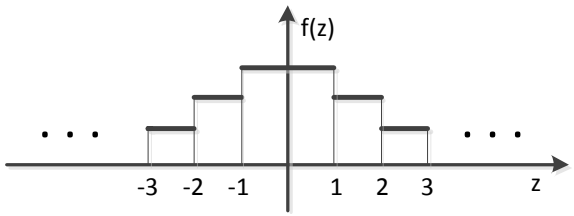


Fig. 1. The staircase-shaped PDF guarantees that $\mathcal{A}$ is $\log(\frac{1}{\varrho})$-differentially private.

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

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

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 (i.e., using (7) as the PDF and setting $\varrho=\frac{1}{e^\epsilon}$ and $a=1$) for the adding noise such that $\mathcal{A}$ is ϵ-differentially private. Meanwhile, it is noted from [3] that given the privacy constraint, the optimal noise probability distribution has a staircase-shaped probability density function in terms of minimizing the data publishing cost (where the cost function is symmetric and increasing). The detailed shape depends on the cost function, and both the length and height of the stairs are different from (7). On the other hand, using Theorem 3.1, for any staircase noise design, it is not difficult to calculate the value of the privacy parameter ϵ, and then verify whether the privacy constraint is satisfied or not. In a word, the staircase-shaped noise is a good choice for the random noise adding mechanism in the application.

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

Theorem 3.3: If $\mathcal{A}$ is ϵ-differentially private, then $\forall i\in V$, there $\nexists\ c_o\in(-\infty,+\infty)$, such that

$$\lim_{z\to c_0} f_{\theta_i}(z)=0.\tag{8}$$

Clearly, (8) is actually a necessary condition of c_2, which can be easily proved by contradiction. This further explains why (8) is necessary to ϵ-differential privacy.

Theorem 3.4: $\mathcal{A}$ is ϵ-differentially private with $\epsilon=\log(c_b)$, if, $\forall i\in V$, there exists a positive constant c_b such that

$$\sup_{\hat{\sigma}\in[-\sigma,\sigma]}\frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)}=c_b.\tag{9}$$

Note that (9) is a stronger condition than conditions c_1 and c_2. Thus, (9) is a sufficient but not necessary condition.

For the above three theorems, all the conditions only depend on the property of the noise distribution function. One can use them to verify the ϵ-differential privacy of the mechanism easily. This is different from most of the existing results in the literature that proved the privacy of the mechanism based on the original definition.

B. 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 3.5: If (6) holds, then $\mathcal{A}$ is (ϵ,δ)-differentially private, where ϵ and δ satisfy $\epsilon=\log(c_b)$ and

$$\delta=\max_{i\in V}\oint_{\Phi_i^0} f_{\theta_i}(z+\sigma)\mathrm{d}z.\tag{10}$$

Moreover, if (5) holds, $\delta=0$, i.e., $\mathcal{A}$ is ϵ-differentially private.

From Theorem 3.5, it is known that (6) is a sufficient condition of (ϵ,δ)-differential privacy. However, it should be pointed out that (6) 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 (6) 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 Gaussian noise ensures (ϵ,δ)-differential privacy.

Theorem 3.6: Let $\Theta=\Theta_0\cup\Theta_1$. Assume that

$$\oint_{\Theta_0} f_{\theta_i}(z)\mathrm{d}z\leq\delta,\forall i\in V\tag{11}$$

and (6) holds when $\theta\in\Theta_1$, i.e.,

$$\sup_{\hat{\sigma}\in[-\sigma,\sigma],\theta\in\Theta_1}\frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)}=c_b.\tag{12}$$

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

Considering the conditions in Theorem 3.6, 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 3.6 that using any kinds of random noise, $\mathcal{A}$ is $(0,1)$-differentially private. This can also shown from the fact that

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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSP.2020.3006760, IEEE Transactions on Signal Processing

holds for any kinds of noise adding mechanism (because $0 \leq \Pr\{\cdot\} \leq 1$ 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

$$\oint_{\Theta_0(k)} f_{\theta_i}(z)\mathrm{d}z \leq \oint_{\Theta_0(k+1)} f_{\theta_i}(z)\mathrm{d}z \leq \oint_{\Theta_0(\infty)} f_{\theta_i}(z)\mathrm{d}z = 1$$

while

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

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 3.5, 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.

C. 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 2.3, it is not obvious to analyze its differential privacy directly from the definition. But, from Theorem 3.3, we easily infer that it is not ϵ-differentially private, since $\lim_{z\to 0} f_{\theta_i}(0) = 0$, 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 and c_2, respectively.

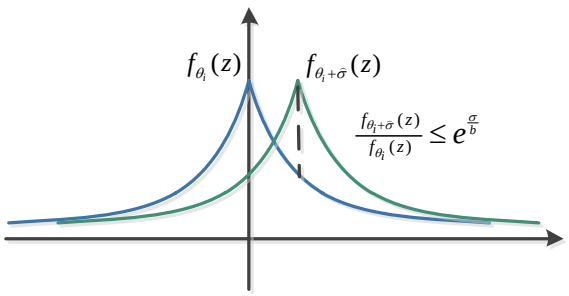


Fig. 2. Laplacian noise: ϵ-differentially private.

From Fig. 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

$$\left|\frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)}\right| = \frac{\frac{1}{2b}e^{-\frac{|z-\hat{\sigma}-a|}{b}}}{\frac{1}{2b}e^{-\frac{|z-a|}{b}}} = e^{\frac{|z-a|-|z-\hat{\sigma}-a|}{b}} \leq e^{\frac{|\sigma|}{b}}.$$

It means that c_2 condition also holds true. Hence, from Theorem 3.1, it follows that Laplacian noise is an ϵ-differentially private noise, where $\epsilon = \log e^{\frac{|\sigma|}{b}} = \frac{|\sigma|}{b}$.

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

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

which means that

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

Hence, from Theorem 3.1, it follows that Gaussian noise is not an ϵ-differentially private noise. However, as shown in Fig. 3,

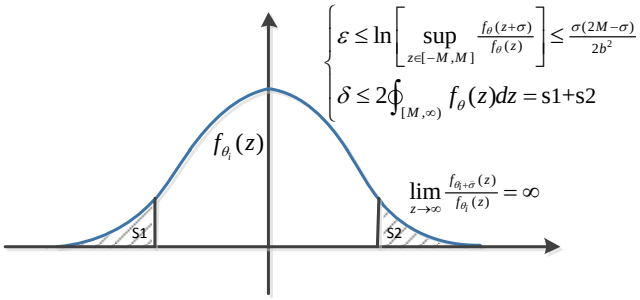


Fig. 3. Gaussian noise: (ϵ,δ)-differentially private.

there exists a large constant M such that ϵ is bounded by

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

for $z\in[-M,M]$, and δ is bounded by

$$\delta \leq \oint_{(-\infty,-M]\cup[M,\infty)} f_{\theta_i}(z)\mathrm{d}z = \frac{1}{b\sqrt{2\pi}}\oint_{(-\infty,-M]\cup[M,\infty)} e^{-\frac{(z-a)^2}{2b^2}}\mathrm{d}z, \quad (13)$$

which is a small value. It means that the conditions in Theorem 3.6 can be satisfied. Thus, we infer from Theorem 3.5 that Gaussian noise is an (ϵ,δ)-differentially private noise, where $\epsilon = \log\frac{\sigma(2M-\sigma)}{2b^2}$ and δ satisfies (13). For Example 2.4, although it is hard to prove its DP from the definition, similar to the above analysis, one infers that condition c_2 of Theorem 3.1 cannot be satisfied. Thus, the mixed Gaussian distribution

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSP.2020.3006760, IEEE Transactions on Signal Processing

noise given in this example cannot guarantee ϵ-differentially privacy.

Lastly, consider the uniform distribution noise with its PDF as $\frac{1}{b-a}$. Clearly, c_1 is not true due to the zero-point set includes continuous interval. Hence, uniform distribution is not an ϵ-differentially private noise. Then, we check the conditions in Theorem 3.5. As shown in Fig. 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 3.5 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.

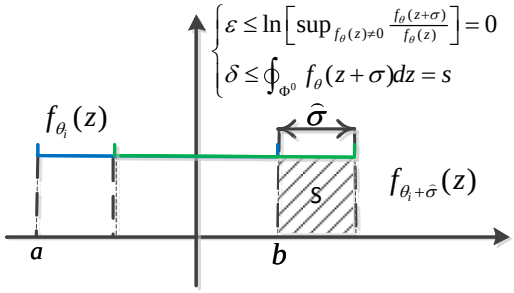


Fig. 4. Uniform noise: $(0, \delta)$-differentially private.

Remark 3.7: The above analysis shows that our method can determine the differential privacy of the randomized mechanism with any given distribution (even the closed-form of the distribution is unknown) of noise by checking the conditions, and thus it is an efficient criterion of differential privacy analysis. This is the main advantage of the propose method. Meanwhile, using our theory 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. More importantly, it should be pointed out that using the propose theory, we can also obtain the values of ϵ and δ directly. This is the other advantage of our method.

IV. 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 [16]–[18]. Consensus algorithm has been applied in a variety of areas, e.g., distributed energy management [19], scheduling [20], and clock synchronization [21]–[23]. 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 [24], [28], [30]. The basic idea is to add random noises to the real state value during the communication for privacy preservation, the same as (3). This motivates us to adopt the developed theories in the above section to analyze differential privacy of the privacy-preserving consensus algorithm.

A. 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 $x(0) = [x_1(0), ..., x_n(0)]^T \in \Omega_x^0 \subseteq \mathbf{R}^n$.

For a general consensus algorithm, each node will communicate with its neighbor nodes and update its state based on the received information. The iteration equation is

$$x_i(k+1) = w_{ii}x_i(k) + \sum_{j\in N_i} w_{ij}x_j(k), \forall i \in V, \tag{14}$$

which can be written in the matrix form as

$$x(k+1) = Wx(k), \tag{15}$$

where w_{ii} and w_{ij} are weights, and W is the weight matrix. It is well known from [35] 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 (15), i.e.,

$$\lim_{k\to\infty} x(k) = \frac{\sum_{\ell=1}^n x_\ell(0)}{n}\mathbf{1} = \bar{x}. \tag{16}$$

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 [30]. Hence, we introduce a common privacy-preserving consensus algorithm as follows:

$$\mathcal{PC}: \begin{cases} x^+(k) = x(k) + \theta(k) \\ x(k+1) = Wx^+(k) \end{cases} \tag{17}$$

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 (16) is achieved under (17).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSP.2020.3006760, IEEE Transactions on Signal Processing

B. Privacy Conditions of Consensus

We define the input and the output sequences of each node i in privacy-preserving consensus algorithm (17) until iteration k as

$$\mathcal{I}_{x_i}^{in}(k) = \{x_i(0), \theta_i(0), ..., \theta_i(k)\}, \tag{18}$$

and

$$\mathcal{I}_{x_i}^{out}(k) = \{x_i^+(0), ..., x_i^+(k)\}, \tag{19}$$

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 $\text{Ra}(\mathcal{PC}) = \Omega_x^0 \oplus \Theta(0) \oplus ... \oplus \Theta(k) \oplus ...$, where $\oplus$ denotes the plus of two sets.

By referring to [28], we introduce the definition of (ϵ, δ)-differential privacy for a consensus algorithm as follows.

Definition 4.1: A PC algorithm (17) is (ϵ, δ)-differentially private if, for any pair x and y of σ-adjacent initial state vector and any set $\mathcal{O} \subseteq \mathbf{R}^{n\times\infty}$,

$$\Pr\{\mathcal{I}_x^{out}(\infty) \in \mathcal{O}\} \leq e^{\epsilon} \Pr\{\mathcal{I}_y^{out}(\infty) \in \mathcal{O}\} + \delta. \tag{20}$$

If $\delta = 0$, we say that (17) is ϵ-differentially private.

First, we give the necessary condition of ϵ-differential privacy for algorithm (17).

Theorem 4.2: If algorithm (17) 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.

Then, the sufficient conditions of differential privacy for algorithm (17) is obtained in the following theorem.

Theorem 4.3: Suppose that the added 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 (17) provides ϵ-differential privacy; if $\theta(0)$ satisfies (6) or (both (11) and (12) simultaneously), algorithm (17) provides (ϵ, δ)-differential privacy, where $\epsilon = \log(c_b)$ and δ satisfies (11).

C. Privacy Analysis of PC Algorithms

We first give the necessary condition of average consensus for algorithm (17).

Theorem 4.4: Using algorithm (17), if

$$\Pr\{\lim_{k\to\infty} x(k) = \bar{x}\} = 1, \tag{21}$$

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 $k \to \infty$.

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

Impossibility Result: From Theorem 4.4, 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

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

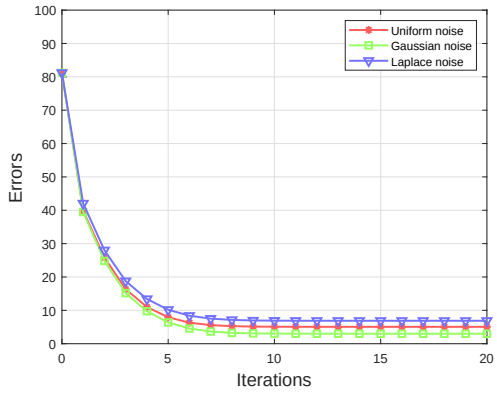
Thus, the conditions c_1 and c_2 no longer hold for the added noise $\sum_{l=0}^{k} W^{k-l}\theta(l)$ when $k \to \infty$. It contradicts with the necessary condition in Theorem 4.2, and thus ϵ-differential privacy cannot be guaranteed. It means that the necessary condition of differential privacy and the necessary condition of average consensus are conflicted, which leads to the impossibility result. Hence, using (17), nodes cannot simultaneously converge to the average of their initial states and preserve ϵ-differential privacy of their initial states.

The above impossibility result is proved by using the conditions of differential privacy given in Theorem 3.1. It can also be proved from the original definition of differential privacy, see [28]. From our proof, however, it is found that the necessary condition of differential privacy and the necessary condition of average consensus are conflicted, which leads to the impossibility result.

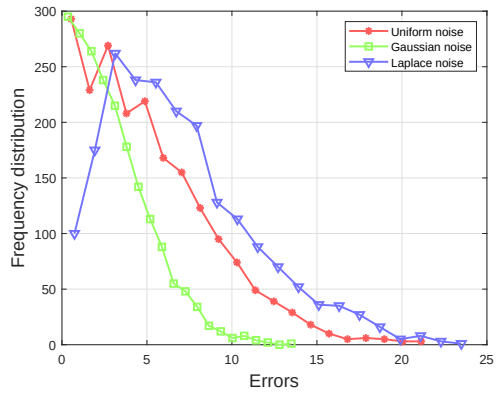
Also, it is not difficult to analyze differential privacy of the existing privacy-preserving consensus algorithm. For example, in [26], [28], the privacy-preserving consensus algorithms are designed by adding independent and Laplacian noise to the consensus process, and thus the sufficient conditions in Theorem 4.3 are satisfied. Hence, these privacy-preserving consensus algorithms proposed in [26], [28] are ϵ-differentially private, while the exact average consensus cannot be guaranteed by these algorithms. In [30], 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 4.2 cannot be satisfied. Hence, the algorithm proposed in [30] 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. It means that the system parameters, e.g., topology parameter, link weights, are also important to state privacy. Katewa et al., in [38] have concerned the privacy of topology and eigenvalues of the network, and designed the novel noise adding mechanism to ensure the privacy. However, what the fundamental relationships among these system parameters, system dynamics, and the state privacy, and the tradeoff among them, are still open issues.

Next, we conduct the simulation to compare the performance of consensus using different noises. Figure 5 compares the performance of the consensus algorithm by adding normal distributed, uniformly distributed, and Laplace distributed noises, respectively. Where the noises are with zero mean and exponentially decaying variance (decay ration is 0.9), and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSP.2020.3006760, IEEE Transactions on Signal Processing



(a) The convergence of the consensus under noises adding.



(b) The error between statble state and average.

Fig. 5. The consensus performance under different noise adding mechanisms.

added independently in each iteration. It is not difficult to prove the convergence of the consensus algorithm with such noises referring the results in existing work, e.g., [30], [31]. However, as shown in Fig. 5(a), it is found that the error between the nodes' states and the average will not converge to zero, i.e., $\lim_{k\to\infty}\sum_{i\in V} \mid x_i(k)-\bar{x} \mid \neq 0$. Then, $1,000$ simulation runs are conducted. The results are shown in Fig. 5(a). It is observed that adding Laplace distribution noise resulting in the worst performance in terms of the convergence accuracy (where the accuracy is defined by $\lim_{k\to\infty}\sum_{i\in V} \mid x_i(k)-\bar{x} \mid$), since it has the highest frequency distribution within the large error interval. However, from Theorem 4.3, adding Laplace noise can ensure ϵ-differential privacy while normal and uniformly noises cannot, i.e., Laplace noise ensure the strongest privacy. Therefore, it is a tradeoff between the privacy and the convergence accuracy.

Remark 4.5: In this paper, the differential privacy is considered in open-loop systems. Considering the differential privacy in closed-loop control systems, it becomes more difficult since the added noise will be involuted in the feedback which may change the system stability, observability, and the controllability. How to design the noise to maintain these performance while ensuring the differential privacy, is challenging and still open, and thus needs extensive further research. In a specific system, if we can quantify how the system dynamics and outputs change the distribution or decrease the uncertainty of the noise, then we can use the obtained theorems to analyze the privacy of the system states.

V. 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], [27], dynamic systems [24] and more. There are also some other privacy definitions, e.g., identifiability and mutual-information privacy, and we refer the readers to [36] for the relationship among 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 [15]. 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 [24]. Wasserman and Zhou in [34] proposed a statistical framework for differential privacy, where the differential privacy is investigated from a statistical perspective. Nissim et al. in [37] 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 and its applications [13], [14], [39], [40]. Theoretically, the objective is to guarantee that the agents' initial states (or objective functions) are private and the average consensus is achieved [24], [26]–[30], [32]. In [27], the authors solved distributed consensus problems while keeping the agents' objective functions private, and in [26] 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. [28] 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. More recently, the privacy issue was concerned in cloud-based control [40], and Akyol et al., [41] have considered the privacy in game theory. Hence, more and

more researchers have paid attention on the privacy different theories and applications.

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.

VI. 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.

Appendix A
Proof for Theorem 3.1

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

First, we prove that (5) is a necessary condition. Assume that there exists an interval $[a, b]$ such that (5) holds for one i_0. Then, there $\exists$ interval $[a, b]$, s.t.,

$$f_{\theta_{i_0}}(z) = 0, \text{ for } z \in [a, b]; f_{\theta_{i_0}}(z) > 0, \text{ for } z \in [b, c] \quad (22)$$

with $c > b$ or $f_{\theta_{i_0}}(z) > 0$ for $z \in [c, a]$ with $a > c$. Without loss of generality, suppose $f_{\theta_i}(z) > 0$ holds for $z \in [b, c]$ in the following proof.

Since the set of all possible values of every node's state at least contains an almost surely continuous interval, i.e., Ω is not a discrete set, it follows that there exists a pair of σ-adjacent state vector, x and y, satisfying $x_{i_0} = y_{i_0} - \sigma_1$ and $x_i = y_i$ (when $i \neq i_0$), where $0 < \sigma_1 \leq b - a$ and $\sigma_1 \leq \sigma$. With (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 $\mathcal{O}_{i_0} \subseteq \mathrm{Ra}(\mathcal{A}(x_{i_0}))$. From (22), it follows that

$$\begin{aligned}
&\Pr\{\mathcal{A}(x_{i_0}) \in \mathcal{O}_{i_0}\} = \int_{y_{i_0}+a}^{y_{i_0}+b} f_{x_{i_0}+\theta_{i_0}}(z)\mathrm{d}z \\
=&\int_{y_{i_0}+a-x_{i_0}}^{y_{i_0}+b-x_{i_0}} f_{\theta_{i_0}}(z)\mathrm{d}z = \int_{a+\sigma_1}^{b+\sigma_1} f_{\theta_{i_0}}(z)\mathrm{d}z \\
=&\int_{a+\sigma_1}^{b} f_{\theta_{i_0}}(z)\mathrm{d}z + \int_{b}^{b+\sigma_1} f_{\theta_{i_0}}(z)\mathrm{d}z \\
\geq&\int_{b}^{b+\sigma_1} f_{\theta_{i_0}}(z)\mathrm{d}z > 0,
\end{aligned}$$

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

$$\begin{aligned}
&\frac{\Pr\{\mathcal{A}(x) \in \mathcal{O}\}}{\Pr\{\mathcal{A}(y) \in \mathcal{O}\}} \\
=&\frac{\Pr\{\mathcal{A}(x_{i_0}) \in \mathcal{O}_{i_0}\}\prod_{i=1,i\neq i_0}^{n}\Pr\{\mathcal{A}(x_i) \in \mathcal{O}_i\}}{\Pr\{\mathcal{A}(y_{i_0}) \in \mathcal{O}_{i_0}\}\prod_{i=1,i\neq i_0}^{n}\Pr\{\mathcal{A}(y_i) \in \mathcal{O}_i\}} \\
=&\frac{\Pr\{\mathcal{A}(x_{i_0}) \in \mathcal{O}_{i_0}\}}{\Pr\{\mathcal{A}(y_{i_0}) \in \mathcal{O}_{i_0}\}} = \infty, \qquad (23)
\end{aligned}$$

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 (5) is a necessary condition if $\mathcal{A}$ is ϵ-differentially private.

Second, we prove that (6) is also a necessary condition. Suppose that

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

which means that for any given large constant M, there $\exists$ z_0 and $\hat{\sigma} \in [-\sigma, \sigma]$, s.t., $f_{\theta_i}(z_0) \neq 0$ and

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

We can 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), we have

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

Similar to (23), one infers 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, (8) is also a necessary condition for ϵ-differentially private.

$\Rightarrow$: Next, we prove the sufficiency. Let $\mathcal{O}_i$ be the domain/set of i-th element in $\mathcal{O}$. Under (3), we have

$$\Pr\{\mathcal{A}(x)\in\mathcal{O}\}=\Pr\{x+\theta\in\mathcal{O}\}$$
$$=\Pr\{x_{i_0}+\theta_{i_0}\in\mathcal{O}_{i_0}\}\prod_{i=1,i\neq i_0}^{n}\Pr\{x_i+\theta_i\in\mathcal{O}_i\}\quad(24)$$

and

$$\Pr\{\mathcal{A}(y)\in\mathcal{O}\}=\Pr\{y+\theta\in\mathcal{O}\}$$
$$=\Pr\{y_{i_0}+\theta_{i_0}\in\mathcal{O}_{i_0}\}\prod_{i=1,i\neq i_0}^{n}\Pr\{y_i+\theta_i\in\mathcal{O}_i\}.\quad(25)$$

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

$$\prod_{i=1,i\neq i_0}^{n}\Pr\{x_i+\theta_i\in\mathcal{O}_i\}=\prod_{i=1,i\neq i_0}^{n}\Pr\{y_i+\theta_i\in\mathcal{O}_i\}.\quad(26)$$

Meanwhile, with the condition c_2, it follows

$$\Pr\{x_{i_0}+\theta_{i_0}\in\mathcal{O}_{i_0}\}=\oint_{\mathcal{O}_{i_0}} f_{x_{i_0}+\theta_{i_0}}(z)\mathrm{d}z$$
$$=\oint_{\mathcal{O}_{i_0}} f_{y_{i_0}-\hat{\sigma}+\theta_{i_0}}(z)\mathrm{d}z\leq\oint_{\mathcal{O}_{i_0}} c_b f_{y_{i_0}+\theta_{i_0}}(z)\mathrm{d}z$$
$$=c_b\Pr\{y_{i_0}+\theta_{i_0}\in\mathcal{O}_{i_0}\},\quad(27)$$

where we have used the fact of (6). Substituting (26) and (27) into (24) yields

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

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 increasing with σ. ■

APPENDIX B
PROOF FOR THEOREM 3.3

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 (5) 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 $\hat{\sigma}\leq\frac{c_1-c_0}{2}$ such that

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

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 $\hat{\sigma}(k)\leq\hat{\sigma}$. Based on (3), we have

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

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

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

which implies that $\mathcal{A}$ is not ϵ-differentially private. It leads to a contradiction. Thus, (8) is a necessary condition when $\mathcal{A}$ is ϵ-differentially private, which completes the proof. ■

APPENDIX C
PROOF FOR THEOREM 3.4

Proof: Note that if (9) can guarantee both conditions c_1 and c_2, then this theorem can be proved from Theorem 3.1.

First, we prove that (9) guarantees condition c_2. By comparing (6) and (9), we note that the constraint $f_{\theta_i}(z)\neq 0$ in (6) is removed in (9), which means that (9) provides a more general result than (6). Hence, one infers that condition c_2 is guaranteed by (9) directly.

Then, we prove that (9) 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

$$\sup_{\hat{\sigma}\in[-\sigma,\sigma]}\frac{f_{\theta_i+\hat{\sigma}}(z)}{f_{\theta_i}(z)}\geq\sup_{\hat{\sigma}\in[-\sigma,\sigma]}\frac{f_{\theta_i}(b+\frac{\hat{\sigma}}{2})}{f_{\theta_i}(b-\frac{\hat{\sigma}}{2})}=\infty,\quad(28)$$

which leads to a contradiction. Therefore, we have that c_1 is also true under (9). ■

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSP.2020.3006760, IEEE Transactions on Signal Processing

APPENDIX D
PROOF FOR THEOREM 3.5

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 (24), (25) and (26) still hold true.

First, we consider the case that the condition c_1 is not true. Then, (27) no longer holds but we obtain

$$\begin{aligned}
&\Pr\{x_{i_0} + \theta_{i_0} \in \mathcal{O}_{i_0}\} = \oint_{\mathcal{O}_{i_0}} f_{x_{i_0}+\theta_{i_0}}(z)\mathrm{d}z \\
&= \oint_{\mathcal{O}_{i_0}} f_{y_{i_0}-\sigma+\theta_{i_0}}(z)\mathrm{d}z \leq \oint_{\mathcal{O}_{i_0}} c_b f_{y_{i_0}+\theta_{i_0}}(z)\mathrm{d}z \\
&+ \oint_{\{\Phi^0_{i_0}+y_{i_0}\}\cap\mathcal{O}_{i_0}} f_{y_{i_0}-\sigma+\theta_{i_0}}(z)\mathrm{d}z \\
&\leq c_b \Pr\{y_{i_0} + \theta_{i_0} \in \mathcal{O}_{i_0}\} + \oint_{\{\Phi^0_{i_0}+y_{i_0}\}} f_{y_{i_0}-\sigma+\theta_{i_0}}(z)\mathrm{d}z \\
&\leq c_b \Pr\{y_{i_0} + \theta_{i_0} \in \mathcal{O}_{i_0}\} + \oint_{\Phi^0_{i_0}} f_{\theta_{i_0}}(z+\sigma)\mathrm{d}z, \qquad (29)
\end{aligned}$$

where we have used the fact that $f_{\theta_{i_0}-\sigma}(z) = f_{\theta_{i_0}}(z+\sigma)$. Then, one infers from (24), (25), (26) and (29) that

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

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

Next, if c_1 holds, it is not difficult to obtain that

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

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

APPENDIX E
PROOF FOR THEOREM 3.6

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

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

Thus, we have completed the proof. ∎

APPENDIX F
PROOF FOR THEOREM 4.2

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

$$\begin{aligned}
&\Pr\{\mathcal{I}^{out}_x(\infty) \in \mathcal{O}\} \leq e^{\epsilon} \Pr\{\mathcal{I}^{out}_y(\infty) \in \mathcal{O}\}, \forall \mathcal{O} \subseteq \mathbf{R}^{n\times\infty} \\
\Leftrightarrow &\Pr\{\mathcal{I}^{out}_x(k) \in \mathcal{O}^{n\times k}\} \leq e^{\epsilon} \Pr\{\mathcal{I}^{out}_y(k) \in \mathcal{O}^{n\times k}\}, \qquad (30) \\
&\forall k \geq 0, \mathcal{O}^{n\times k} \subseteq \mathbf{R}^{n\times k} \\
\Rightarrow &\Pr\{x^+(k) \in \mathcal{O}^{n\times 1}\} \leq e^{\epsilon} \Pr\{y^+(k) \in \mathcal{O}^{n\times 1}\}, \qquad (31) \\
&\forall k \geq 0, \mathcal{O}^{n\times k} \subseteq \mathbf{R}^{n\times k}.
\end{aligned}$$

From (17), we have

$$\begin{aligned}
x^+(k) &= x(k) + \theta(k) \\
&= W[x(k-1) + \theta(k-1)] + \theta(k) \\
&= W^k x(0) + \sum_{l=0}^{k} W^{k-l}\theta(l) \\
&= x(0) + (W^k - I)x(0) + \sum_{l=0}^{k} W^{k-l}\theta(l), \qquad (32)
\end{aligned}$$

where I is an identity matrix. From (30), (32) and Theorem 3.1, 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. ∎

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSP.2020.3006760, IEEE Transactions on Signal Processing

APPENDIX G
PROOF FOR THEOREM 4.3

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, (17) provides ϵ-differential privacy.

When $\theta(0)$ satisfies (6), we have

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

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

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

Thus, (17) provides (ϵ, δ)-differential privacy.

If $\theta(0)$ satisfies both (11) and (12) simultaneously, then there also exists Θ_0 and Θ_1 such that $\theta(0)+x$ satisfies (11) and (12). Hence, we have

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

It means that (17) provides (ϵ, δ)-differential privacy.

Thus, we have completed the proof. ■

APPENDIX H
PROOF FOR THEOREM 4.4

Proof: Under algorithm (17), 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 (21), 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 $\Pr\{\lim_{k\to\infty} W\theta(k) = 0\} = 1$. ■

ACKNOWLEDGEMENT

The authors would like to thank the editor and the anonymous reviewers for their constructive comments. The authors would also like to thank Chengcheng Zhao for her discussions on this article. This work is partially supported by the National Key R&D Program of China 2017YFE0114600, and by the Natural Science Foundation of China (NSFC) under grant 61973218, 61828301, and the Natural Sciences and Engineering Research Council of Canada (NSERC).

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 Trans. 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. in *Proc. 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. IEEE CDC*, 2014.

[9] M. Abadi, A. Chu, I. Goodfellow, H. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep Learning with differential privacy," *in Proc. ACM CCS*, 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] C. Zhao, J. Chen, J. He, and P. Cheng. "Privacy-preserving consensus-based energy management in smart grids," *IEEE Trans. Signal Processing*, 66(23): 6162-6176, 2018.

[14] X. Wang, J. He, P. Cheng, and J. Chen. "Privacy preserving collaborative computing: Heterogeneous privacy guarantee and efficient incentive mechanism," *IEEE Trans. Signal Processing*, 67(1): 221-233, 2018.

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

[16] 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.

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

[18] 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.

[19] C. Zhao, J. He, P. Cheng and J. Chen, "Consensus-based energy management in smart grid with transmission losses and directed communication," *IEEE Trans. Smart Grid*, 8(5): 2049-2061,2017.

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

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

[22] 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.

[23] 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.

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

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

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

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

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

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

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

[31] J He, L Cai, P Cheng, J Pan, L Shi, "Consensus-based data-privacy preserving data aggregation," *IEEE Trans. Automat Contr.*, 64 (12): 5222—5229, 2019.

[32] M. Ruan, H. Gao, and Y. Wang, "Secure and privacy-preserving consensus," *IEEE Trans. Automat Contr.*, 64(10): 4035–4049, 2019.

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

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

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

[36] W. Wang, L. Ying, and J. Zhang, "On the relation between identifiability, differential privacy, and mutual-information privacy," *IEEE Trans. Information Theory*, 62(9), 5018-5029, 2017.

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

[38] V. Katewa, A. Chakrabortty, and V. Gupta. "Protecting privacy of topology in consensus networks." in *Proc. IEEE ACC*, 2015.

[39] Y. Liu, J. Liu, and T. Basar. "Differentially private gossip gradient descent." in *Proc. IEEE CDC*, 2018.

[40] T. Tanaka, M. Skoglund, H. Sandberg, and K. Johansson. "Directed information and privacy loss in cloud-based control." in *Proc. IEEE ACC*, 2017.

[41] E. Akyol, C. Langbort, and T. Basar. "Networked estimation-privacy games." in *Proc. IEEE GlobalSIP*, 2017.

Jianping He (M'15-SM'19) is currently an associate professor in the Department of Automation at Shanghai Jiao Tong University. He received the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2013, and had been a research fellow in the Department of Electrical and Computer Engineering at University of Victoria, Canada, from Dec. 2013 to Mar. 2017. His research interests mainly include the distributed learning, control and optimization, security and privacy in network systems.

Dr. He serves as an Associate Editor for IEEE Open Journal of Vehicular Technology and KSII Trans. Internet and Information Systems. He was also a Guest Editor of IEEE TAC, International Journal of Robust and Nonlinear Control, etc. He was the winner of Outstanding Thesis Award, Chinese Association of Automation, 2015. He received the best paper award from IEEE WCSP'17, the best conference paper award from IEEE PESGM'17, and was a finalist for the best student paper award from IEEE ICCA'17.

Lin Cai (S'00-M'06-SM'10-F'20) received her M.A.Sc. and Ph. D. degrees (awarded Outstanding Achievement in Graduate Studies) in electrical and computer engineering from the University of Waterloo, Waterloo, Canada, in 2002 and 2005, respectively. Since 2005, she has been with the Department of Electrical & Computer Engineering at the University of Victoria, and she is currently a Professor. She is an NSERC E.W.R. Steacie Memorial Fellow and an IEEE Fellow. Her research interests span several areas in communications and networking, with a focus on network protocol and architecture design supporting emerging multimedia traffic and the Internet of Things.

She was a recipient of the NSERC Discovery Accelerator Supplement (DAS) Grants in 2010 and 2015, respectively, and the Best Paper Awards of IEEE ICC 2008 and IEEE WCNC 2011. She has co-founded and chaired the IEEE Victoria Section Vehicular Technology and Communications Joint Societies Chapter. She has been elected to serve the IEEE Vehicular Technology Society Board of Governors, 2019 - 2021. She has served as an area editor for IEEE Transactions on Vehicular Technology, a member of the Steering Committee of the IEEE Transactions on Big Data (TBD) and IEEE Transactions on Cloud Computing (TCC), an Associate Editor of the IEEE Internet of Things Journal, IEEE Transactions on Wireless Communications, IEEE Transactions on Vehicular Technology, IEEE Transactions on Communications, EURASIP Journal on Wireless Communications and Networking, International Journal of Sensor Networks, and Journal of Communications and Networks (JCN), and as the Distinguished Lecturer of the IEEE VTS Society. She has served as a TPC co-chair for IEEE VTC2020-Fall, and a TPC symposium co-chair for IEEE Globecom'10 and Globecom'13. She is a registered professional engineer in British Columbia, Canada.

Xinping Guan (SM'04-F'18) is currently a Chair Professor of Shanghai Jiao Tong University, China, where he is the Deputy Director of University Research Management Office, and the Director of the Key Laboratory of Systems Control and Information Processing, Ministry of Education of China. Before that, he was the Professor and Dean of Electrical Engineering, Yanshan University, China.

Dr. Guan's current research interests include industrial cyber-physical systems, wireless networking and applications in smart city and smart factory, and underwater sensor networks. He has authored and/or coauthored 4 research monographs, more than 270 papers in IEEE Transactions and other peer-reviewed journals, and numerous conference papers. As a Principal Investigator, he has finished/been working on many national key projects. He is the leader of the prestigious Innovative Research Team of the National Natural Science Foundation of China (NSFC). Dr. Guan is an Executive Committee Member of Chinese Automation Association Council and the Chinese Artificial Intelligence Association Council. He was elevated to IEEE Fellow in 2017. He received the First Prize of Natural Science Award from the Ministry of Education of China in both 2006 and 2016, and the Second Prize of the National Natural Science Award of China in 2008. He was a recipient of the "IEEE Transactions on Fuzzy Systems Outstanding Paper Award" in 2008. He is a "National Outstanding Youth" honored by NSF of China, "Changjiang Scholar" by the Ministry of Education of China and State-level Scholar of New Century Bai Qianwan Talent Program of China.