

Preserving Data-Privacy with Added Noises: Optimal Estimation and Privacy Analysis

Jianping He^{1,2}, Lin Cai² and Xinping Guan¹

Abstract

Networked systems often relies on distributed algorithms to achieve a global computation goal with iterative local information exchanges between neighbor nodes. To preserve data privacy, a node may add a random noise to its original data for information exchange at each iteration. Nevertheless, a neighbor node can estimate other's original data based on the information it received. The estimation accuracy and data privacy can be measured in terms of (ϵ, δ) -data-privacy, defined as the probability of ϵ -accurate estimation (the difference of an estimation and the original data is within ϵ) is no larger than δ (the disclosure probability). How to optimize the estimation and analyze data privacy is a critical and open issue. In this paper, a theoretical framework is developed to investigate how to optimize the estimation of neighbor's original data using the local information received, named optimal distributed estimation. Then, we study the disclosure probability under the optimal estimation for data privacy analysis. We further apply the developed framework to analyze the data privacy of the privacy-preserving average consensus algorithm and identify the optimal noises for the algorithm.

Index Terms

Distributed algorithm, Noise adding mechanism, Distributed estimation, Data privacy, Average consensus.

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, xpguan@sjtu.edu.cn

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

The preliminary result of this work was submitted to IEEE Conference on Decision and Control (CDC), 2017.

I. INTRODUCTION

Without relying on a central controller, distributed algorithms are robust and scalable, so they have been widely adopted in networked systems to achieve global computation goals (e.g., mean and variance of the distributed data) with iterative local information exchanges between neighbor nodes [1]–[3]. In many scenarios, e.g., social networks, the nodes’ original data may include users’ private or sensitive information, e.g., age, income, daily activities, and opinions. With the privacy concern, nodes in the network may not be willing to share their real data with others. To preserve data privacy, a typical method is adding random noises to the data to be released in each iteration. With the noise adding procedure, the goal of privacy-preserving distributed algorithms is to ensure data privacy while achieving the global computation goal [4]–[6].

Consensus, an efficient distributed computing and control algorithm, has been heavily investigated and widely applied, e.g., in distributed estimation and optimization [8], [9], distributed energy management and scheduling [10], [11], and time synchronization in sensor networks [12]–[14]. Recently, the privacy-preserving average consensus problem has attracted attention, aiming to guarantee that the privacy of the initial states is preserved while an average consensus can still be achieved [15]–[19]. The main solution is to add variance decaying and zero-sum random noises during each iteration of the consensus process.

In the literature, differential privacy, a formal mathematical standard, has been defined and applied for quantifying to what extent individual privacy in a statistical database is preserved [20]. It aims to provide means to maximize the accuracy of queries from statistical databases while maintaining indistinguishability of its transcripts. To guarantee the differential privacy, a commonly used noise is Laplacian noise [21], [22].

Different from the database query problems, for many distributed computing algorithms such as consensus, the key privacy concern is to ensure that other nodes cannot accurately estimate the original data, instead of the indistinguishability. No matter what type of noise distribution is used, there is a chance that an estimated value of the original data is close to the real data, such a probability cannot be directly measured by differential privacy. To quantify the estimation accuracy and data privacy, we first define ϵ -accurate estimation, i.e., the difference of the estimated value and the original data is no larger than ϵ . We then define (ϵ, δ) -data-privacy in [6] as that the probability of ϵ -accurate estimation is no larger than δ . Using the

(ϵ, δ) -data-privacy definition, in this paper, we develop a theoretical framework to investigate how to optimize the estimation of neighbor's original data using the local information received, named optimal distributed estimation. Then, we study the disclosure probability under the optimal estimation for data privacy analysis. The main contributions of this work are summarized as follows.

- 1) To the best of our knowledge, this is the first work to mathematically formulate and solve the optimal distributed estimation problem and data privacy problem for the distributed algorithm with a general noise adding mechanism. The optimal distributed estimation is defined as the estimation that can achieve the highest disclosure probability, δ , of ϵ -accurate estimation, given the available information set.
- 2) A theoretical framework is developed to analyze the optimal distributed estimation and data privacy by considering the distributed algorithm with a noise adding procedure, where the closed-form solutions of both the optimal distributed estimation and the privacy parameter are obtained. The obtained results show that how the iteration process and the noise adding sequence affect the estimation accuracy and data privacy, which reveals the relationship among noise distribution, estimation and data privacy.
- 3) We apply the obtained theoretical framework to analyze the privacy of a general privacy-preserving average consensus algorithm (PACA), and quantify the (ϵ, δ) -data-privacy of PACA. We also identify the condition that the data privacy may be compromised. We further obtain the optimal noise distribution for PACA under which the disclosure probability of ϵ -accurate estimation is minimized, i.e., the highest data privacy is achieved.

The rest of this paper is organized as follows. Section II provides preliminaries and formulates the problem. The optimal distributed estimation and the privacy analysis under different available information set are discussed in Sections III and IV, respectively. In Section V, we apply the framework to analyze the data privacy of PACA. Concluding remarks and further research issues are given in Section VI.

II. PRELIMINARIES PROBLEM FORMULATION

A networked system is abstracted as an undirected and connected graph, denoted by $G = (V, E)$, where V is the set of nodes and E is the set of edges. An edge $(i, j) \in E$ exists if and only if (iff) nodes i can exchange information with node j . Let $N_i = \{j | (i, j) \in E\}$ be the

TABLE I
IMPORTANT NOTATIONS

| Symbol | Definition |
|--------------------------|--|
| G | the network graph |
| $x_i(0)$ | node i 's initial state |
| $x(0)$ | the initial state vector of all nodes |
| $f_i(\cdot)$ | the distributed iteration algorithm |
| Θ_i | the domain of random variable θ_i |
| $f_{\theta_i}(\cdot)$ | the PDF of random variable θ_i |
| $\mathcal{I}_i^{in}(k)$ | the noise input of node i until iteration k |
| $\mathcal{I}_i^{out}(k)$ | the information output of node i until iteration k |
| $\hat{x}_i^*(k)$ | the optimal distributed estimation of $x_i(0)$ until iteration k |
| ϵ | the measure on estimation accuracy |
| δ | the disclosure probability |
| \mathcal{I}_ν^{out} | the possible output when the initial input is ν |
| $\mathcal{I}_j^i(k)$ | the information available to node j to estimate $x_i(0)$ until iteration k |

neighbor set of node i ($i \notin N_i$). Let $n = |V|$ be the total number of nodes and $n \geq 3$. Each node i in the network has an initial scalar state $x_i(0) \in \mathcal{R}$, which can be any type of data, e.g., the sensed or measured data of the node. Let $x(0) = [x_1(0), \dots, x_n(0)]^T \in \mathcal{R}^n$ be the initial state vector.

A. Privacy-Preserving Distributed Algorithm

The goal of a distributed algorithm is to obtain the statistics of all nodes' initial states (e.g., the average, maximum, or minimum value, variance, etc.) in a distributed manner. Nodes in the network use the local information exchange to achieve the goal, and thus each node will communicate with its neighbor nodes periodically for data exchange and state update. With the privacy concerns, each node is not willing to release its real initial state to its neighbor nodes. A widely used approach for the privacy preservation is adding random noises at each iteration for local data exchange.

Define $x_i^+(k)$ the data being sent out by node i in iteration k , given by

$$x_i^+(k) = x_i(k) + \theta_i(k), \quad (1)$$

where $\theta_i(k) \in \Theta_i$ is a random variable. When node i receives the information from its neighbor nodes, it updates its state using the following function,

$$x_i(k+1) = f_i(x_i^+(k), x_j^+(k) : j \in N_i), \quad (2)$$

where the state-transition function, $f_i : \mathcal{R} \times \mathcal{R} \times \dots \times \mathcal{R} \rightarrow \mathcal{R}$, depends on $x_i^+(k)$ and $x_j^+(k)$ for $j \in N_i$ only. The above equation defines a distributed iteration algorithm with privacy preserving since only the neighbor nodes' information is used for state update in each iteration and the data exchanged have been mixed with random noises to preserve privacy. Hence, (2) is named as a privacy-preserving distributed algorithm. Since the initial state is most important for each node in the sense of privacy, in this paper, we focus on the estimation and privacy analysis of nodes' initial states.

B. Important Notations and Definitions

Define the noise input and state/information output sequences of node i in the privacy-preserving distributed algorithm until iteration k by

$$\mathcal{I}_i^{in}(k) = \{\theta_i(0), \dots, \theta_i(k)\}, \quad (3)$$

and

$$\mathcal{I}_i^{out}(k) = \{x_i^+(0), \dots, x_i^+(k)\}, \quad (4)$$

respectively. Note that for any neighbor node j , it can not only receive the information output $I_i^{out}(k)$ of node i , but also eavesdrop the information output of all their common neighbor nodes, which means that there may be more information available for node j to estimate $x_i(0)$ at iteration $k \geq 1$. Hence, we define

$$I_j^i(k) = \{x_i^+(0), x_\ell^+(0), \dots, x_i^+(k), x_\ell^+(k) \mid \\ \ell = j \text{ or } \ell \in N_i \cap N_j\},$$

as the available information set/outputs for node j to estimate $x_i(0)$ of node i at iteration k . Clearly, we have $I_i^{out}(0) = I_j^i(0)$ and $I_i^{out}(k) \subseteq I_j^i(k)$.

Let $f_{\theta_i(k)}(z)$ be the probability density function (PDF) of random variable $\theta_i(k)$. Let $\mathcal{X}_i \subseteq \mathcal{R}$ be the set of the possible values of $x_i(0)$. Clearly, if $\mathcal{X}_i = \mathcal{R}$, it means that $x_i(0)$ can be any

value in \mathcal{R} . Given any function $f(y)$, we define the function $f(y, \epsilon)$ as

$$f(y, \epsilon) = f(y + \epsilon) - f(y - \epsilon), \quad (5)$$

and let

$$\Omega_f^0 = \{y | f(y, \epsilon) = 0\} \quad (6)$$

be the zero-point set of $f(y, \epsilon) = 0$. Let $\{\circ\}_b$ be the boundary point set of a given set $\{\circ\}$, e.g., $(0, 1]_b = \{0, 1\}$.

Note that each node can estimate its neighbor nodes' initial states based on all the information it knows, i.e., the available information set of the node. For example, based on $I_j^i(0) = x_i^+(0)$, node j can take the probability over the space of noise $\theta_i(0)$ (where the space is denoted by $\Theta_i(0)$) to estimate the values of the added noises, and then infer the initial state of node i using the difference between $x_i^+(0)$ and the real initial state $x_i(0)$, i.e., $\hat{x}_i(0) = x_i^+(0) - \hat{\theta}_i(0)$. Hence, we give two definitions for the estimation as follows.

Definition 2.1: Let \hat{x}_i be an estimation of variable x_i . If $|x_i - \hat{x}_i| \leq \epsilon$, where $\epsilon \geq 0$ is a small constant, then we say \hat{x}_i is an ϵ -accurate estimation.

Note that $\mathcal{I}_i^{out}(k)$ is the information output sequence of node i , which is related to $x_i(0)$ directly, and this should be considered in the estimation. Since only the local information is available to the estimation, we define the optimal distributed estimation of $x_i(0)$ as follows.

Definition 2.2: Let $\mathcal{I}_\nu^{out}(k)$ be the possible output given the condition that $x_i(0) = \nu$ at iteration k . Considering ϵ -accurate estimation, under $\mathcal{I}_j^i(k)$,

$$\hat{x}_i^*(k) = \arg \max_{\hat{x}_i \in \mathcal{X}_i} \Pr \{ \mathcal{I}_\nu^{out}(k) = \mathcal{I}_i^{out}(k) \mid \forall |\nu - \hat{x}_i| \leq \epsilon \},$$

is named the optimal distributed estimation of $x_i(0)$ at iteration k . Then, $\hat{x}_i^* = \lim_{k \rightarrow \infty} \hat{x}_i^*(k)$ is named the optimal distributed estimation of $x_i(0)$.

In order to quantify the degree of the privacy protection of the privacy-preserving distributed algorithm and construct a relationship between estimation accuracy and the privacy, we introduce the following (ϵ, δ) -data-privacy definition.

Definition 2.3: A distributed randomized algorithm is (ϵ, δ) -data-private, iff

$$\delta = \Pr \{ |\hat{x}_i^* - x_i(0)| \leq \epsilon \}, \quad (7)$$

where δ is the disclosure probability that the initial state $x_i(0)$ can be successfully estimated by others using the optimal distributed estimation in a given interval $[x_i(0) - \epsilon, x_i(0) + \epsilon]$.

In the above definition, \hat{x}_i^* depends on the output sequences, $\mathcal{I}_i^{out}(k)$, which are the functions of random noise inputs $\mathcal{I}_i^{in}(k)$ and its neighbors' output $\mathcal{I}_j^{out}(k)$, $j \in N_i$. All the possible outputs of $\mathcal{I}_i^{out}(k)$ under a privacy-preserving distributed algorithm should be considered to calculate δ , and thus \hat{x}_i^* is a random variable in (7). There are two important parameters in the privacy definition, ϵ and δ , where ϵ denotes the estimation accuracy and δ is the disclosure probability ($\delta \leq 1$) denoting the degree of the privacy protection. A smaller value of ϵ corresponds to a higher accuracy, and a smaller value of δ corresponds to a lower maximum disclosure probability.

C. Problem of Interests

We have the following basic assumptions, i) if there is no information of any variable y in estimation, then the domain of y is viewed as \mathcal{R} , ii) unless specified, the global topology information is unknown to each node, iii) the initial states of nodes in the network are independent of each other, i.e., each node cannot estimate the other nodes' state directly based on its own state or the estimation is of low accuracy.

In this paper, we aim to provide a theoretical framework of the optimal distributed estimation and data privacy analysis for the privacy-preserving distributed algorithm (2). Specifically, we are interesting in the following three issues: i) how to obtain the optimal distributed estimation and its closed-form expression considering the distributed algorithm (2); ii) using the (ϵ, δ) -data-private definition to analyze the privacy of the distributed algorithm (2), i.e., obtaining the closed-form expression of the disclosure probability δ and its properties; and iii) using the obtained theoretical results to analyze the privacy of the existing privacy-preserving average consensus algorithm, and finding the optimal noise adding process to the algorithm, i.e.,

$$\begin{aligned} & \min_{\mathcal{I}_i^{in}(\infty)} \delta. \\ & s.t. \quad \lim_{k \rightarrow \infty} x_i(k) = \bar{x}, \end{aligned} \tag{8}$$

where $\bar{x} = \frac{\sum_{i=1}^n x_i(0)}{n}$ is the statistic goal, aiming at minimizing the disclosure probability while obtaining the average value of all initial states.

To solve the above issues, in the following, we first consider the case that only the one-step information output ($I_i^{out}(0) = I_j^i(0)$), which depends on the initial state ($x_i(0)$) and the

one-step noise ($\theta_i(0)$), is available, and obtain the optimal distributed estimation and privacy properties. This case is suitable for the general one-step random mechanism (e.g., [23], [26]), and the theoretical results provide the foundations of the following analysis. Then, we consider the optimal distributed estimation under the information set $I_j^i(1)$, which reveals that how the iteration process affects the estimation and helps to understand the optimal distributed estimation under the information set $I_j^i(k)$ ($k \geq 1$). Based on the observations, we extend the results to the general case that $I_j^i(k)$ ($\forall k \geq 0$) is available for the estimation. Lastly, we apply the obtained results to the general PACA algorithm for privacy analysis, and discuss the optimal noises for preserving the data privacy.

III. OPTIMAL DISTRIBUTED ESTIMATION AND PRIVACY ANALYSIS UNDER $I_j^i(0)$

In this section, the optimal distributed estimation of $x_i(0)$ using the information $I_j^i(0)$ only is investigated, and the disclosure probability δ under the optimal estimation is derived.

A. Optimal Distributed Estimation under $I_j^i(0)$

Let $e_{\theta_i(0)}$ be the estimation of $\theta_i(0)$ under $I_j^i(0)$. The optimal distributed estimation of $x_i(0)$ under $I_j^i(0)$ and its closed-form expression are given in the following theorem.

Theorem 3.1: Considering the distributed algorithm (2), under $I_j^i(0)$, the optimal distributed estimation of $x_i(0)$ satisfies

$$\hat{x}_i^*(0) = x_i^+(0) - e_{\theta_i(0)}(x_i^+(0)), \quad (9)$$

where

$$e_{\theta_i(0)}(x_i^+(0)) = \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)}(z) \mathbf{d}z; \quad (10)$$

Specifically, if $\mathcal{X}_i = \mathcal{R}$, then

$$\hat{x}_i^*(0) = x_i^+(0) - e_{\theta_i(0)}, \quad (11)$$

where

$$e_{\theta_i(0)} = \arg \max_{y \in \mathcal{R}} \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)}(z) \mathbf{d}z, \quad (12)$$

which is independent of $x_i^+(0)$.

Proof: Given $I_i^{out}(0)$ and an estimation $\hat{x}_i(0)$, we have

$$\begin{aligned}
& \Pr \{ \mathcal{I}_\nu^{out}(0) = \mathcal{I}_i^{out}(0) \mid \forall |\nu - \hat{x}_i(0)| \leq \epsilon \} \\
&= \Pr \{ \nu + \theta_i(0) = x_i^+(0) \mid \forall |\nu - \hat{x}_i(0)| \leq \epsilon \} \\
&= \int_{x_i^+(0) - \hat{x}_i(0) - \epsilon}^{x_i^+(0) - \hat{x}_i(0) + \epsilon} f_{\theta_i(0)}(z) \mathbf{d}z.
\end{aligned} \tag{13}$$

From Definition 2.2, it follows that

$$\begin{aligned}
\hat{x}_i^*(0) &= \arg \max_{\hat{x}_i(0) \in \mathcal{X}_i} \Pr \{ \mathcal{I}_\nu^{out}(0) = \mathcal{I}_i^{out}(0) \mid \forall |\nu - \hat{x}_i(0)| \leq \epsilon \} \\
&= \arg \max_{\hat{x}_i(0) \in \mathcal{X}_i} \int_{x_i^+(0) - \hat{x}_i(0) - \epsilon}^{x_i^+(0) - \hat{x}_i(0) + \epsilon} f_{\theta_i(0)}(z) \mathbf{d}z \\
&= x_i^+(0) - \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} \int_{y - \epsilon}^{y + \epsilon} f_{\theta_i(0)}(z) \mathbf{d}z \\
&= x_i^+(0) - e_{\theta_i(0)}(x_i^+(0)),
\end{aligned} \tag{14}$$

which concludes that (9) holds.

If $\mathcal{X}_i = \mathcal{R}$, for any real number output of $x_i^+(0)$, we have

$$\{x_i^+(0) - \mathcal{X}_i\} = \{x_i^+(0) - \mathcal{R}\} = \mathcal{R}.$$

In this case, we have

$$\begin{aligned}
& \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} \int_{y - \epsilon}^{y + \epsilon} f_{\theta_i(0)}(z) \mathbf{d}z \\
&= \arg \max_{y \in \mathcal{R}} \int_{y - \epsilon}^{y + \epsilon} f_{\theta_i(0)}(z) \mathbf{d}z.
\end{aligned} \tag{15}$$

Substituting (15) into (14) gives

$$\begin{aligned}
\hat{x}_i^*(0) &= x_i^+(0) - \arg \max_{y \in \mathcal{R}} \int_{y - \epsilon}^{y + \epsilon} f_{\theta_i(0)}(z) \mathbf{d}z \\
&= x_i^+(0) - e_{\theta_i(0)},
\end{aligned}$$

i.e., (11) holds. Thus, we have completed the proof. ■

In (9), $e_{\theta_i(0)}(x_i^+(0))$ can be viewed as the estimation of the noise $\theta_i(0)$, i.e., $\hat{\theta}_i(0) = e_{\theta_i(0)}(x_i^+(0))$.

Thus, (9) can be written as

$$\hat{x}_i^*(0) = x_i^+(0) - \hat{\theta}_i(0),$$

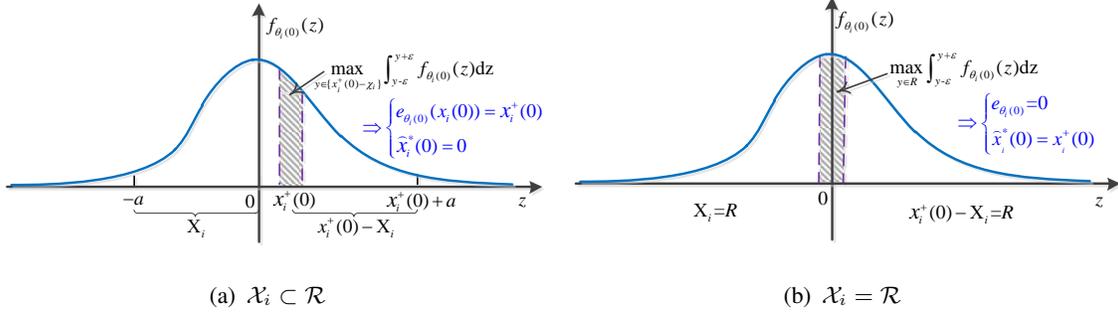


Fig. 1. Two examples of the optimal distributed estimation under $I_i^{out}(0)$ considering $\mathcal{X}_i \subset \mathcal{R}$ and $\mathcal{X}_i = \mathcal{R}$, respectively.

which means that the estimation problem is equivalent to estimating the value of the added noise. From (10), it is noted that $e_{\theta_i(0)}(x_i^+(0))$ depends on ϵ , $x_i^+(0)$, $f_{\theta_i(0)}$ and \mathcal{X}_i . We use Fig. 1(a) as an example to illustrate how to obtain $e_{\theta_i(0)}(x_i^+(0))$ and $\hat{x}_i^*(0)$ when $\mathcal{X}_i \subset \mathcal{R}$. Let the blue curve be the $f_{\theta_i(0)}(z)$ (it follows the Gaussian distribution in this example) and $\mathcal{X}_i = [-a, 0]$, and $x_i^+(0)$ is the fixed initial output. We then have

$$x_i^+(0) - \mathcal{X}_i = [x_i^+(0), x_i^+(0) + a].$$

Given an ϵ and $y \in [x_i^+(0), x_i^+(0) + a]$, $\int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)}(z)dz$ denotes the shaded area of $f_{\theta_i(0)}(z)$ in the interval $[y-\epsilon, y+\epsilon]$, which is named as the ϵ -shaded area of $f_{\theta_i(0)}(z)$ at point y . Clearly, when $y = x_i^+(0)$, $f_{\theta_i(0)}(z)$ has the largest ϵ -shaded area. It follows that $e_{\theta_i(0)}(x_i^+(0)) = x_i^+(0)$, and thus $\hat{x}_i^*(0) = 0$. Meanwhile, we consider the case that $\mathcal{X}_i = \mathcal{R}$ or \mathcal{X}_i is not available to the other nodes, and use Fig. 1(b) as an example for illustration. In this case, we have $\mathcal{X}_i = x_i^+(0) - \mathcal{X}_i = \mathcal{R}$ for any output $x_i^+(0)$. From the above theorem, we have

$$e_{\theta_i(0)}(x_i^+(0)) = e_{\theta_i(0)} = \arg \max_{y \in \mathcal{R}} \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)}(z)dz = 0.$$

Then, the optimal distributed estimation $\hat{x}_i^*(0) = x_i^+(0) - 0 = x_i^+(0)$ given any output $x_i^+(0)$.

Next, a general approach is introduced to calculate the value of $e_{\theta_i(0)}(x_i^+(0))$. Note that

$$\begin{aligned} \frac{\partial(\int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)}(z)dz)}{\partial y} &= F_{\theta_i(0)}(y+\epsilon) - F_{\theta_i(0)}(y-\epsilon) \\ &= F_{\theta_i(0)}(y, \epsilon). \end{aligned}$$

It is well known that $F_{\theta_i(0)}(y, \epsilon) = 0$ is a necessary condition that y is an extreme point of $\int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)}(z)dz$. One then follows from (10) that $e_{\theta_i(0)}(x_i^+(0))$ is either one of the extreme points

of $\int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)}(z)dz$ (i.e., $e_{\theta_i(0)}(x_i^+(0)) \in \Omega_{F_{\theta_i(0)}}^0$) or one of the boundary points of $\{x_i^+(0) - \mathcal{X}_i\}$ (i.e., $e_{\theta_i(0)}(x_i^+(0)) \in \{x_i^+(0) - \mathcal{X}_i\}_b$). Let

$$\mathcal{X}_{x_i^+(0)} = \{x_i^+(0) - \mathcal{X}_i\} \cap \Omega_{F_{\theta_i(0)}}^0 \cup \{x_i^+(0) - \mathcal{X}_i\}_b,$$

we then have

$$e_{\theta_i(0)}(x_i^+(0)) = \arg \max_{y \in \mathcal{X}_{x_i^+(0)}} \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)}(z)dz. \quad (16)$$

Applying the above general approach to the example of Fig. 1, one can easily obtain that

$$\mathcal{X}_{x_i^+(0)} = \{x_i^+(0), x_i^+(0) + a\}$$

and $\mathcal{X}_{x_i^+(0)} = \{0\}$ for the two cases, respectively. Based on (16), we obtain the same optimal estimations for the two cases.

Remark 3.2: From the above discussion, it is observed that $e_{\theta_i(0)}(x_i^+(0))$ is the point y that $f_{\theta_i(0)}(z)$ has the largest ϵ -shaded area around point y , where $y \in \{x_i^+(0) - \mathcal{X}_i\}$. It should be pointed out that $e_{\theta_i(0)}(x_i^+(0))$ is in $\{x_i^+(0) - \mathcal{X}_i\}$ and depends on ϵ , and thus it may not be the point that has the maximum value of $f_{\theta_i(0)}(z)$. However, if ϵ is sufficiently small and $f_{\theta_i(0)}(z)$ is continuous, $f_{\theta_i(0)}(z)$ typically has the largest ϵ -shaded area at point y when $f_{\theta_i(0)}(y)$ has the maximum value for $y \in \{x_i^+(0) - \mathcal{X}_i\}$. Meanwhile, the above examples also show that the unbiased estimation also may not be the optimal distributed estimation of $x_i(0)$.

B. Privacy Analysis under $I_j^i(0)$

In the above subsection, we have obtained the optimal distributed estimation when $I_i^{out}(0)$ is fixed. Note that

$$\begin{aligned} |\hat{x}_i^*(0) - x_i(0)| &\leq \epsilon \\ \Leftrightarrow |x_i^+(0) - x_i(0) - e_{\theta_i(0)}(x_i^+(0))| &\leq \epsilon \\ \Leftrightarrow |\theta_i(0) - e_{\theta_i(0)}(x_i^+(0))| &\leq \epsilon \end{aligned} \quad (17)$$

when $x_i^+(0)$ is fixed. To analyze the privacy of distributed algorithm (2) with the (ϵ, δ) -data-privacy definition, the main goal is to calculate the disclosure probability δ , so that all the possible initial output $x_i^+(0)$ and its corresponding optimal distributed estimation should be considered.

Considering the outputs which can make an ϵ -accurate estimations of $x_i(0)$ to be obtained, we define all the corresponding noises by

$$\mathcal{S}_i(0) = \{\theta_i(0) \mid |e_{\theta_i(0)}(x_i^+(0)) - \theta_i(0)| \leq \epsilon\}. \quad (18)$$

For each $\theta_i(0) \in \mathcal{S}_i(0)$, we have $x_i^+(0) = x_i(0) + \theta_i(0)$ and $|e_{\theta_i(0)}(x_i^+(0)) - \theta_i(0)| \leq \epsilon$, i.e., an ϵ -accurate estimation is obtained when $\theta_i(0) \in \mathcal{S}_i(0)$.

Theorem 3.3: Considering the distributed algorithm (2), under $I_j^i(0)$, the disclosure probability δ satisfies

$$\delta = \oint_{\mathcal{S}_i(0)} f_{\theta_i(0)}(z) \mathbf{d}z; \quad (19)$$

Specifically, if $\mathcal{X}_i = \mathcal{R}$, then

$$\delta = \max_{y \in \mathcal{R}} \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)}(z) \mathbf{d}z. \quad (20)$$

Proof: From (17) and the definition of δ , we have

$$\begin{aligned} \delta &= \Pr\{|\hat{x}_i^*(0) - x_i(0)| \leq \epsilon\} \\ &= \Pr\{|\theta_i(0) - e_{\theta_i(0)}(x_i^+(0))| \leq \epsilon\} \\ &= \Pr\{\theta_i(0) \in \mathcal{S}_i(0)\} \\ &= \oint_{\mathcal{S}_i(0)} f_{\theta_i(0)}(z) \mathbf{d}z. \end{aligned} \quad (21)$$

From Theorem 3.1, if $\mathcal{X}_i = \mathcal{R}$, then $e_{\theta_i(0)}(x_i^+(0)) = e_{\theta_i(0)}$ which is independent of $x_i^+(0)$. In this case, we have

$$\begin{aligned} \mathcal{S}_i(0) &= \{\theta_i(0) \mid |e_{\theta_i(0)} - \theta_i(0)| \leq \epsilon\} \\ &= [e_{\theta_i(0)} - \epsilon, e_{\theta_i(0)} + \epsilon], \end{aligned} \quad (22)$$

i.e., only if $\theta_i(0) \in [e_{\theta_i(0)} - \epsilon, e_{\theta_i(0)} + \epsilon]$, we can obtain the ϵ -accurate estimation of $x_i(0)$. Then,

$$\begin{aligned} \delta &= \oint_{\mathcal{S}_i(0)} f_{\theta_i(0)}(z) \mathbf{d}z \\ &= \int_{e_{\theta_i(0)} - \epsilon}^{e_{\theta_i(0)} + \epsilon} f_{\theta_i(0)}(z) \mathbf{d}z. \end{aligned} \quad (23)$$

Since $e_{\theta_i(0)}$ satisfies (12), $e_{\theta_i(0)}$ is the point y that $f_{\theta_i(0)}(z)$ has the largest ϵ -shaded area around it, and the domain of y is \mathcal{R} . It follows that

$$\begin{aligned}\delta &= \int_{e_{\theta_i(0)} - \epsilon}^{e_{\theta_i(0)} + \epsilon} f_{\theta_i(0)}(z) \mathbf{d}z \\ &= \max_{y \in \mathcal{R}} \int_{y - \epsilon}^{y + \epsilon} f_{\theta_i(0)}(z) \mathbf{d}z.\end{aligned}\quad (24)$$

We thus have completed the proof. ■

From the above theorem, we obtain that (19) provides the expression of the disclosure probability δ under $I_i^{out}(0)$. Using (19), the main challenge to calculate δ is that how to obtain the set of $\mathcal{S}_i(0)$. Although based on the definition of $\mathcal{S}_i(0)$, the elements of $\mathcal{S}_i(0)$ can be obtained by comparing all possible values of $\theta_i(0)$ and their corresponding $e_{\theta_i(0)}(x_i^+(0))$ (how to obtain the value of $e_{\theta_i(0)}(x_i^+(0))$ is discussed in the previous subsection), this approach is infeasible due to the infinite possible values of $\theta_i(0)$. Fortunately, we can apply the properties of $f_{\theta_i(0)}$ to fast obtain $\mathcal{S}_i(0)$ in many cases of practical importance. For the example given in Fig. 1(a), since $f_{\theta_i(0)}$ is continuous and concave, it is straight-forward to obtain that

$$e_{\theta_i(0)}(x_i^+(0)) = \begin{cases} x_i^+(0), & x_i^+(0) \geq 0; \\ 0, & x_i^+(0) \in [-a, 0]; \\ x_i^+(0) + a, & x_i^+(0) \leq -a. \end{cases}$$

Using the facts that $\hat{x}_i^*(0) = x_i^+(0) - e_{\theta_i(0)}(x_i^+(0))$ and $x_i^+(0) = x_i(0) + \theta_i(0)$, we then obtain

$$\hat{x}_i^*(0) - x_i(0) = \begin{cases} -x_i(0), & x_i(0) + \theta_i(0) \geq 0; \\ \theta_i(0), & x_i(0) + \theta_i(0) \in [-a, 0]; \\ -a - x_i(0), & x_i(0) + \theta_i(0) \leq -a. \end{cases}$$

Based on the above equation, for any given $x_i(0)$ and ϵ , we obtain all the $\theta_i(0)$ in $\mathcal{S}_i(0)$ by solving $|\hat{x}_i^*(0) - x_i(0)| \leq \epsilon$, and thus $\mathcal{S}_i(0)$ is obtained.

IV. OPTIMAL DISTRIBUTED ESTIMATION AND PRIVACY UNDER $I_j^i(k)$

In this section, we investigate the optimal distributed estimation and privacy under $I_j^i(1)$, and then extend the results to the general case that $I_j^i(k)$ is available to the estimation. Let $e_{\theta_i(0)|I_j^i(k)}$ be the estimation of $\theta_i(0)$ under $I_j^i(k)$.

A. Optimal Distributed Estimation under $I_j^i(1)$

Under $I_j^i(1)$, there are two outputs, $x_i^+(0)$ and $x_i^+(1)$, of node i , which can be used for initial state estimation or inference attack. Note that $x_i^+(1) = f_i(x_i^+(0), x_j^+(0) : j \in N_i)$, which means that $x_i^+(1)$ has involved the outputs of node i 's neighbors. Hence, under $I_j^i(1)$, both the optimal distributed estimation and privacy analysis depend on the output of both node i and its neighbor nodes. Suppose that f_i in (2) is available to the estimation in the remainder parts of this paper.

The following theorem provides the optimal distributed estimation of $x_i(0)$ under $I_j^i(1)$, which reveals the relationship between the information outputs (which are available to the node j for estimation) and the optimal estimation.

Theorem 4.1: Considering the distributed algorithm (2), under $I_j^i(1)$, the optimal distributed estimation of $x_i(0)$ satisfies

$$\hat{x}_i^*(1) = x_i^+(0) - e_{\theta_i(0)|I_j^i(1)}(x_i^+(0)), \quad (25)$$

where

$$e_{\theta_i(0)|I_j^i(1)}(x_i^+(0)) = \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(1)}(\theta_i'(1)) f_{\theta_i(0)|\theta_i(1)=\theta_i'(1)}(z) \mathbf{d}z, \quad (26)$$

in which $\theta_i'(1) = x_i^+(1) - f_i(x_i^+(0), x_j^+(0) : j \in N_i)$; Then, if $\mathcal{X}_i = \mathcal{R}$, we have

$$e_{\theta_i(0)|I_j^i(1)}(x_i^+(0)) = \arg \max_{y \in \mathcal{R}} \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(1)}(\theta_i'(1)) f_{\theta_i(0)|\theta_i(1)=\theta_i'(1)}(z) \mathbf{d}z. \quad (27)$$

Proof: Let $\hat{x}_i(1)$ be an estimation of $x_i(0)$ under $I_j^i(1)$ at iteration $k = 1$. Given $\mathcal{I}_i^{out}(1)$, and we have

$$\begin{aligned} & \Pr\{\mathcal{I}_\nu^{out}(1) = \mathcal{I}_i^{out}(1) \mid \forall |\nu - \hat{x}_i(1)| \leq \epsilon, I_j^i(1)\} \\ &= \Pr\{\mathcal{I}_\nu^{out}(1) = \{x_i^+(0), x_i^+(1)\} \mid \forall |\nu - \hat{x}_i(1)| \leq \epsilon, I_j^i(1)\}. \end{aligned}$$

Note that $x_i^+(0)$ depends on $x_i(0)$ and $\theta_i(0)$ only, while $x_i^+(1)$ depends on $x_i^+(0), x_j^+(0) : j \in N_i$

and $\theta_i(1)$, where $\theta_i(0)$ and $\theta_i(1)$ are two random variables. It follows that

$$\begin{aligned}
& \Pr\{\mathcal{I}_\nu^{out}(1) = \{x_i^+(0), x_i^+(1)\} \mid \forall |\nu - \hat{x}_i(1)| \leq \epsilon, I_j^i(1)\} \\
&= \Pr\{\mathcal{I}_\nu^{out}(0, 0) = x_i^+(0), \mathcal{I}_i^{out}(0, 1) = x_i^+(1) \mid \\
&\quad \forall |\nu - \hat{x}_i(1)| \leq \epsilon, I_j^i(1)\} \\
&= \int_{\hat{x}_i(1)-\epsilon}^{\hat{x}_i(1)+\epsilon} f_{\theta_i(0), \theta_i(1)}(x_i^+(0) - \nu, \theta_i'(1)) \mathbf{d}\nu,
\end{aligned} \tag{28}$$

where

$$\theta_i'(1) = x_i^+(1) - f_i(x_i^+(0), x_j^+(0) : j \in N_i).$$

Using the relationship between the joint distribution and the conditional distribution, one infers that

$$\begin{aligned}
& \int_{\hat{x}_i(1)-\epsilon}^{\hat{x}_i(1)+\epsilon} f_{\theta_i(0), \theta_i(1)}(x_i^+(0) - \nu, \theta_i'(1)) \mathbf{d}\nu \\
&= \int_{x_i^+(0)-\hat{x}_i(1)-\epsilon}^{x_i^+(0)-\hat{x}_i(1)+\epsilon} f_{\theta_i(1)}(\theta_i'(1)) f_{\theta_i(0)|\theta_i(1)}(z|\theta_i(1) = \theta_i'(1)) \mathbf{d}z \\
&= \int_{x_i^+(0)-\hat{x}_i(1)-\epsilon}^{x_i^+(0)-\hat{x}_i(1)+\epsilon} f_{\theta_i(1)}(\theta_i'(1)) f_{\theta_i(0)|\theta_i(1)=\theta_i'(1)}(z) \mathbf{d}z
\end{aligned} \tag{29}$$

where $f_{\theta_i(0)|\theta_i(1)=\theta_i'(1)}$ is the conditional PDF of $\theta_i(0)$ under the condition $\theta_i(1) = \theta_i'(1)$. Then, one can obtain that

$$\begin{aligned}
& \max_{\hat{x}_i \in \mathcal{X}_i} \Pr\{\mathcal{I}_\nu^{out}(k) = \mathcal{I}_i^{out}(k) \mid \forall |\nu - \hat{x}_i| \leq \epsilon, I_j^i(1)\} \\
&= \max_{\hat{x}_i \in \mathcal{X}_i} \int_{x_i^+(0)-\hat{x}_i(1)-\epsilon}^{x_i^+(0)-\hat{x}_i(1)+\epsilon} f_{\theta_i(1)}(\theta_i'(1)) f_{\theta_i(0)|\theta_i(1)=\theta_i'(1)}(z) \mathbf{d}z.
\end{aligned} \tag{30}$$

Hence, we have

$$\begin{aligned}
\hat{x}_i^*(1) &= \arg \max_{\hat{x}_i \in \mathcal{X}_i} \int_{x_i^+(0)-\hat{x}_i(1)-\epsilon}^{x_i^+(0)-\hat{x}_i(1)+\epsilon} \\
&\quad f_{\theta_i(1)}(\theta_i'(1)) f_{\theta_i(0)|\theta_i(1)=\theta_i'(1)}(z) \mathbf{d}z \\
&= x_i^+(0) - e_{\theta_i(0)|I_j^i(k)}(x_i^+(0)).
\end{aligned}$$

When $\mathcal{X}_i = \mathcal{R}$, we have $x_i^+(0) - \mathcal{X}_i = \mathcal{R}$ holds for any output $x_i^+(0) \in \mathcal{R}$. It follows that (26) is equivalent to (27) in this case. Thus, the proof is completed. \blacksquare

Note that the joint distribution of any two random variables X and Y satisfies

$$f_{X,Y}(x,y) = f_{X|Y}(x|y)f_Y(y) = f_{Y|X}(y|x)f_X(x), \quad (31)$$

and we have

$$\begin{aligned} & \int_{\hat{x}_i(1)-\epsilon}^{\hat{x}_i(1)+\epsilon} f_{\theta_i(0),\theta_i(1)}(x_i^+(0) - \nu, \theta'_i(1)) \mathbf{d}\nu \\ &= \int_{x_i^+(0)-\hat{x}_i(1)-\epsilon}^{x_i^+(0)-\hat{x}_i(1)+\epsilon} f_{\theta_i(1)|\theta_i(0)}(\theta'_i(1)|\theta_i(0) = z) f_{\theta_i(0)}(z) \mathbf{d}z \\ &= \int_{x_i^+(0)-\hat{x}_i(1)-\epsilon}^{x_i^+(0)-\hat{x}_i(1)+\epsilon} f_{\theta_i(1)|\theta_i(0)=z}(\theta'_i(1)) f_{\theta_i(0)}(z) \mathbf{d}z. \end{aligned} \quad (32)$$

It thus follows that $e_{\theta_i(0)|I_j^i(1)}(x_i^+(0))$ also satisfies

$$\begin{aligned} & e_{\theta_i(0)|I_j^i(1)}(x_i^+(0)) \\ &= \arg \max_{y \in \mathcal{R}} \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(1)|\theta_i(0)=z}(\theta'_i(1)) f_{\theta_i(0)}(z) \mathbf{d}z. \end{aligned} \quad (33)$$

It should be noticed that $e_{\theta_i(0)|I_j^i(1)}(x_i^+(0))$ can be viewed as the optimal distributed estimation of $\theta_i(0)$ under $I_j^i(1)$, which depends on the distributions of $\theta_i(1)$ and $\theta_i(0)$, the values of $x_i^+(0)$ and $\theta'_i(1)$, and \mathcal{X}_i . Next, we consider how these factors affect the value of $e_{\theta_i(0)|I_j^i(1)}(x_i^+(0))$.

Corollary 4.2: Considering the distributed algorithm (2), if $\theta_i(0)$ and $\theta_i(1)$ are independent of each other, under $I_j^i(1)$, we have $e_{\theta_i(0)|I_j^i(1)}(x_i^+(0)) = e_{\theta_i(0)}(x_i^+(0))$ and the optimal distributed estimation of $x_i(0)$ satisfies

$$\hat{x}_i^*(1) = \hat{x}_i^*(0) = x_i^+(0) - e_{\theta_i(0)}(x_i^+(0)). \quad (34)$$

Proof: For $e_{\theta_i(0)|I_j^i(1)}(x_i^+(0))$ in (25), since $\theta_i(0)$ and $\theta_i(1)$ are independent of each other, we have that

$$f_{\theta_i(1)|\theta_i(0)}(\theta'_i(1)|\theta_i(0) = z) = f_{\theta_i(1)}(\theta'_i(1)) \quad (35)$$

holds for $\forall z$. Then, it follows from (31) that

$$\begin{aligned}
& \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(1)}(\theta'_i(1)) f_{\theta_i(0)|\theta_i(1)=\theta'_i(1)}(z) \mathbf{d}z \\
&= \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(1)|\theta_i(0)}(\theta'_i(1)|\theta_i(0)=z) f_{\theta_i(0)}(z) \mathbf{d}z \\
&= \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(1)}(\theta'_i(1)) f_{\theta_i(0)}(z) \mathbf{d}z \\
&= f_{\theta_i(1)}(\theta'_i(1)) \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)}(z) \mathbf{d}z, \tag{36}
\end{aligned}$$

where $f_{\theta_i(1)}(\theta'_i(1))$ is a constant when $I_j^i(1)$ is fixed. Together with (26), one infers that

$$\begin{aligned}
& e_{\theta_i(0)|I_j^i(1)}(x_i^+(0)) \\
&= \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} \left(f_{\theta_i(1)}(\theta'_i(1)) \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)}(z) \mathbf{d}z \right) \\
&= \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)}(z) \mathbf{d}z \\
&= e_{\theta_i(0)}(x_i^+(0)), \tag{37}
\end{aligned}$$

where we use the fact that $f_{\theta_i(1)}(\theta'_i(1))$ is a constant under $I_j^i(1)$. From Theorem 4.1, we have known that under $I_j^i(1)$, $\hat{x}_i^*(1)$ satisfies (25). Substituting (37) into (25), one obtains (34), which completes the proof. \blacksquare

The above corollary shows that when the added noises are independent of each other, the optimal distributed estimation $e_{\theta_i(0)|I_j^i(1)}(x_i^+(0))$ of $\theta_i(0)$ at iteration $k = 1$ equals the optimal distributed estimation $e_{\theta_i(0)}(x_i^+(0))$ of $\theta_i(0)$ at iteration $k = 0$, and thus we have $\hat{x}_i^*(1) = \hat{x}_i^*(0)$. Hence, one concludes that the later outputs cannot increase the estimation accuracy of $x_i(0)$ when the added noise sequence are independent of each other, and more details related to this conclusion will be provided in the next subsection.

Corollary 4.3: Considering the distributed algorithm (2), if $N_i \not\subseteq N_j$ for $\forall j \in N_i$ or the other nodes do not know all the information used for the updating by node i , under $I_j^i(1)$, the optimal distributed estimation of $x_i(0)$ satisfies

$$\hat{x}_i^*(1) = x_i^+(0) - e'_{\theta_i(0)|I_j^i(1)}(x_i^+(0)), \tag{38}$$

where

$$e'_{\theta_i(0)|I_j^i(1)}(x_i^+(0)) = \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} \int_{y-\epsilon}^{y+\epsilon} \oint_{\Theta_{\theta_i'(1)|I_j^i(1)}} f_{\theta_i(1)}(h) f_{\theta_i(0)|\theta_i(1)=h}(z) \mathbf{d}h \mathbf{d}z, \quad (39)$$

and $\Theta_{\theta_i'(1)|I_j^i(1)}$ is the set of all possible values of $\theta_i'(1)$ under $I_j^i(1)$. Specifically, if $\Theta_{\theta_i'(1)|I_j^i(1)} \supseteq \Theta_i(1)$, we have $e'_{\theta_i(0)|I_j^i(1)}(x_i^+(0)) = e_{\theta_i(0)}(x_i^+(0))$ and $\hat{x}_i^*(1) = \hat{x}_i^*(0)$.

Proof: For $\forall j \in N_i$, since $N_i \not\subseteq N_j$, there is at least one neighbor node of node i satisfying $l \in N_i$ but $l \notin N_j$. It means that node j cannot obtain all the neighbor nodes' information used for node i 's state updating. Thus, in the expression of $\theta_i'(1)$, there is at least one unknown variable in $f_i(x_i^+(0), x_j^+(0) : j \in N_i)$, which results that the exact value of $\theta_i'(1)$ cannot be obtained. Hence, during the estimation, $\theta_i'(1)$ is no longer a deterministic value but is in a possible value set. Let $\Theta_{\theta_i'(1)|I_j^i(1)}$ be set of the all possible values of $\theta_i'(1)$ under $I_j^i(1)$. During the estimation, we take all possible values of $\theta_i'(1)$ into consideration, and then obtain

$$\begin{aligned} & \Pr\{\mathcal{I}_\nu^{out}(1) = \{x_i^+(0), x_i^+(1)\} \mid \forall |\nu - \hat{x}_i(1)| \leq \epsilon, I_j^i(1)\} \\ &= \int_{x_i^+(0) - \hat{x}_i(1) - \epsilon}^{x_i^+(0) - \hat{x}_i(1) + \epsilon} \oint_{\Theta_{\theta_i'(1)|I_j^i(1)}} f_{\theta_i(1)}(h) \mathbf{d}h f_{\theta_i(0)|\theta_i(1)=h}(z) \mathbf{d}z. \end{aligned}$$

Therefore, we have

$$\begin{aligned} \hat{x}_i^*(1) &= \arg \max_{\hat{x}_i \in \mathcal{X}_i} \Pr\{\mathcal{I}_\nu^{out}(1) = \{x_i^+(0), x_i^+(1)\} \mid \\ & \quad \forall |\nu - \hat{x}_i(1)| \leq \epsilon, I_j^i(1)\} \\ &= x_i^+(0) - \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} \int_{y-\epsilon}^{y+\epsilon} \oint_{\Theta_{\theta_i'(1)|I_j^i(1)}} \\ & \quad f_{\theta_i(1)}(h) \mathbf{d}h f_{\theta_i(0)|\theta_i(1)=h}(z) \mathbf{d}z \\ &= x_i^+(0) - e'_{\theta_i(0)|I_j^i(k)}(x_i^+(0)). \end{aligned}$$

If $\Theta_{\theta'_i(1)|I_j^i(1)} \supseteq \Theta_i(1)$, we have

$$\begin{aligned} & \int_{y-\epsilon}^{y+\epsilon} \oint_{\Theta_{\theta'_i(1)|I_j^i(1)}} f_{\theta_i(1)}(h) \mathbf{d}h f_{\theta_i(0)|\theta_i(1)=h}(z) \mathbf{d}z \\ &= \int_{y-\epsilon}^{y+\epsilon} \oint_{\Theta_i(1)} f_{\theta_i(1)|\theta_i(0)=z}(h) \mathbf{d}h f_{\theta_i(0)}(z) \mathbf{d}z \\ &= \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)}(z) \mathbf{d}z, \end{aligned}$$

where we have used the fact that

$$\oint_{\Theta_i(1)} f_{\theta_i(1)|\theta_i(0)=z}(h) \mathbf{d}h \equiv 1$$

holds for $\forall z \in \mathcal{R}$. It thus has

$$\begin{aligned} e'_{\theta_i(0)|I_j^i(k)}(x_i^+(0)) &= \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)}(z) \mathbf{d}z \\ &= e_{\theta_i(0)}(x_i^+(0)), \end{aligned}$$

which means that

$$\hat{x}_i^*(1) = x_i^+(0) - e_{\theta_i(0)}(x_i^+(0)) = \hat{x}_i^*(0).$$

We thus have completed the proof. ■

In the above corollary, if the assumption that for an unknown variable, it can be any value in \mathcal{R} for estimation and $f_i(x_i^+(0), x_j^+(0) : j \in N_i)$ with domain \mathcal{R} , then we have $\Theta_{\theta'_i(1)|I_j^i(1)} = \mathcal{R}$ since there is at least one unknown variable in $f_i(x_i^+(0), x_j^+(0) : j \in N_i)$. Then, (48) can be simplified to

$$\begin{aligned} & e'_{\theta_i(0)|I_j^i(1)}(x_i^+(0)) \\ &= \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} \int_{y-\epsilon}^{y+\epsilon} \oint_{\mathcal{R}} f_{\theta_i(1)}(h) f_{\theta_i(0)|\theta_i(1)=h}(z) \mathbf{d}h \mathbf{d}z \\ &= \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} \int_{y-\epsilon}^{y+\epsilon} \oint_{\mathcal{R}} f_{\theta_i(1)|\theta_i(0)=z}(h) \mathbf{d}h f_{\theta_i(0)}(z) \mathbf{d}z \\ &= \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)}(z) \mathbf{d}z, \end{aligned}$$

where we have used the facts that (31) and

$$\int_{y-\epsilon}^{y+\epsilon} \oint_{\mathcal{R}} f_{\theta_i(1)|\theta_i(0)=z}(h) \mathbf{d}h \equiv 1.$$

Corollary 4.4: Considering the distributed algorithm (2), if $N_i \subseteq N_j$ and N_i are known to node j , under $I_j^i(1)$, the optimal distributed estimation of $x_i(0)$ satisfies (25) with

$$e_{\theta_i(0)|I_j^i(1)}(x_i^+(0)) = \arg \max_{y \in \mathcal{R}} \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)|\theta_i(1)=\theta_i'(1)}(z) \mathbf{d}z.$$

Proof: When $N_i \subseteq N_j$ and N_i are known to node j , under $I_j^i(1)$, node j can obtain the exact value of $\theta_i'(1)$, since all the information of $x_i^+(1) - f_i(x_i^+(0), x_j^+(0)) : j \in N_i$ are available to it. That is, $\theta_i'(1)$ is fixed when node j makes the estimation, and thus

$$\begin{aligned} & \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(1)}(\theta_i'(1)) f_{\theta_i(0)|\theta_i(1)=\theta_i'(1)}(z) \mathbf{d}z \\ &= \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)|\theta_i(1)=\theta_i'(1)}(z) \mathbf{d}z. \end{aligned} \quad (40)$$

Then, from Theorem 4.1, we can obtain the results given in this corollary, which has completed the proof. \blacksquare

Corollaries 4.3 and 4.4 show the optimal distributed estimation of $x_i(0)$ until iteration k , considering node j can and cannot have all information of the parameters in $f_i(x_i^+(0), x_j^+(0)) : j \in N_i$ for the estimation, respectively. Therefore, they reveal that how the neighbor nodes' information outputs affect the optimal distributed estimation according to the iteration process of the privacy-preserving distributed algorithm (2).

B. Optimal Distributed Estimation under $I_j^i(k)$

In this subsection, we consider the optimal distributed estimation of $x_i(0)$ under $I_j^i(k)$. Let $k \rightarrow \infty$, and we obtain the optimal distributed estimation under $I_j^i(\infty)$.

We first give the following theorem, which provides the expression of the optimal distributed estimation under $I_j^i(k)$.

Theorem 4.5: Considering the distributed algorithm (2), under $I_j^i(k)$, the optimal distributed estimation of $x_i(0)$ satisfies

$$\hat{x}_i^*(k) = x_i^+(0) - e_{\theta_i(0)|I_j^i(k)}(x_i^+(0)), \quad (41)$$

where

$$\begin{aligned}
& e_{\theta_i(0)|I_j^i(k)}(x_i^+(0)) \\
&= \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(1), \dots, \theta_i(k)}(\theta_i'(1), \dots, \theta_i'(k)) \\
& \quad f_{\theta_i(0)|\theta_i(k)=\theta_i'(k), \dots, \theta_i(1)=\theta_i'(1)}(z) \mathbf{d}z, \tag{42}
\end{aligned}$$

in which $\theta_i'(k) = x_i^+(k) - f_i(x_i^+(k-1), x_j^+(k-1) : j \in N_i)$.

Proof: From Theorem 4.1, it is proved that (41) holds for $k = 1$. Now, we prove that it holds for $\forall k \geq 1$, where the basic idea is similar to the proof of Theorem 4.1.

Let $\hat{x}_i(k)$ be an estimation of $x_i(0)$ under $I_j^i(k)$. We have the following equation holds,

$$\begin{aligned}
& \Pr \{ \mathcal{I}_\nu^{\text{out}}(k) = \mathcal{I}_i^{\text{out}}(k) \mid \forall |\nu - \hat{x}_i(k)| \leq \epsilon, I_j^i(k) \} \\
&= \Pr \{ \mathcal{I}_\nu^{\text{out}}(k) = \{x_i^+(0), \dots, x_i^+(k)\} \mid \forall |\nu - \hat{x}_i(k)| \leq \epsilon, I_j^i(k) \} \\
&= \Pr \{ \mathcal{I}_\nu^{\text{out}}(0, 0) = x_i^+(0), \dots, \mathcal{I}_i^{\text{out}}(k-1, k) = x_i^+(k) \mid \\
& \quad \forall |\nu - \hat{x}_i(k)| \leq \epsilon, I_j^i(k) \} \\
&= \int_{\hat{x}_i(k)-\epsilon}^{\hat{x}_i(k)+\epsilon} f_{\theta_i(0), \dots, \theta_i(k)}(x_i^+(0) - \nu, \theta_i'(1), \dots, \theta_i'(k)) \mathbf{d}\nu,
\end{aligned}$$

where

$$\theta_i'(k) = x_i^+(k) - f_i(x_i^+(k-1), x_j^+(k-1) : j \in N_i).$$

Using the properties of the joint distribution of multiple random variables, one infers that

$$\begin{aligned}
& \int_{\hat{x}_i(k)-\epsilon}^{\hat{x}_i(k)+\epsilon} f_{\theta_i(0), \dots, \theta_i(k)}(x_i^+(0) - \nu, \theta_i'(1), \dots, \theta_i'(k)) \mathbf{d}\nu \\
&= \int_{x_i^+(0)-\hat{x}_i(k)-\epsilon}^{x_i^+(0)-\hat{x}_i(k)+\epsilon} f_{\theta_i(1), \dots, \theta_i(k)}(\theta_i'(1), \dots, \theta_i'(k)) \\
& \quad f_{\theta_i(0)|\{\theta_i(1), \dots, \theta_i(k)\}}(z|\theta_i'(1), \dots, \theta_i'(k)) \mathbf{d}z \\
&= \int_{x_i^+(0)-\hat{x}_i(k)-\epsilon}^{x_i^+(0)-\hat{x}_i(k)+\epsilon} f_{\theta_i(1), \dots, \theta_i(k)}(\theta_i'(1), \dots, \theta_i'(k)) \\
& \quad f_{\theta_i(0)|\theta_i(k)=\theta_i'(k), \dots, \theta_i(1)=\theta_i'(1)}(z) \mathbf{d}z \tag{43}
\end{aligned}$$

where $f_{\theta_i(0)|\theta_i(k)=\theta'_i(k),\dots,\theta_i(1)=\theta'_i(1)}(z)$ is the conditional PDF of $\theta_i(0)$ under the condition that $\{\theta_i(k) = \theta'_i(k), \dots, \theta_i(1) = \theta'_i(1)\}$. Then, one obtains that

$$\begin{aligned}
\hat{x}_i^*(1) &= \arg \max_{\hat{x}_i \in \mathcal{X}_i} \Pr\{\mathcal{I}_\nu^{out}(k) = \mathcal{I}_i^{out}(k) \mid \\
&\quad \forall |\nu - \hat{x}_i(k)| \leq \epsilon, I_j^i(k)\} \\
&= \arg \max_{\hat{x}_i \in \mathcal{X}_i} \int_{x_i^+(0) - \hat{x}_i(k) - \epsilon}^{x_i^+(0) - \hat{x}_i(k) + \epsilon} f_{\theta_i(1), \dots, \theta_i(k)}(\theta'_i(1), \dots, \theta'_i(k)) \\
&\quad f_{\theta_i(0)|\theta_i(k)=\theta'_i(k), \dots, \theta_i(1)=\theta'_i(1)}(z) \mathbf{d}z \\
&= x_i^+(0) - \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} f_{\theta_i(1), \dots, \theta_i(k)}(\theta'_i(1), \dots, \theta'_i(k)) \\
&\quad f_{\theta_i(0)|\theta_i(k)=\theta'_i(k), \dots, \theta_i(1)=\theta'_i(1)}(z) \mathbf{d}z \\
&= x_i^+(0) - e_{\theta_i(0)|I_j^i(k)}(x_i^+(0)). \tag{44}
\end{aligned}$$

Thus, the proof is completed. ■

Then, we study the optimal distributed estimation of $x_i(0)$ under $I_j^i(k)$ and some other conditions, and provide three corollaries, respectively, as follows.

Corollary 4.6: Considering the distributed algorithm (2), if the added noises $\theta_i(0), \dots, \theta_i(k)$ are independent of each other, under $I_j^i(k)$, $e_{\theta_i(0)|I_j^i(k)}(x_i^+(0)) = e_{\theta_i(0)}(x_i^+(0))$ and the optimal distributed estimation of $x_i(0)$ satisfies

$$\hat{x}_i^*(k) = \hat{x}_i^*(0) = x_i^+(0) - e_{\theta_i(0)}(x_i^+(0)). \tag{45}$$

Proof: We only need to prove $e_{\theta_i(0)|I_j^i(k)}(x_i^+(0)) = e_{\theta_i(0)}(x_i^+(0))$, then (45) can be inferred from Theorem 4.5 directly. Since the added noises are independent of each other, we have

$$f_{\theta_i(0)|\theta_i(k)=\theta'_i(k), \dots, \theta_i(1)=\theta'_i(1)}(z) = f_{\theta_i(0)}(z).$$

Then, (42) can be simplified

$$\begin{aligned}
& e_{\theta_i(0)|I_j^i(k)}(x_i^+(0)) \\
&= \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} f_{\theta_i(1), \dots, \theta_i(k)}(\theta'_i(1), \dots, \theta'_i(k)) \\
& \quad \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)}(z) \mathbf{d}z \\
&= \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)}(z) \mathbf{d}z \\
&= e_{\theta_i(0)}(x_i^+(0)), \tag{46}
\end{aligned}$$

which completes the proof. ■

Corollary 4.7: Considering the distributed algorithm (2), if $N_i \not\subseteq N_j$ for $\forall j \in N_i$ or the other nodes do not know all the information used for the updating by node i , under $I_j^i(k)$, the optimal distributed estimation of $x_i(0)$ satisfies

$$\hat{x}_i^*(k) = x_i^+(0) - e'_{\theta_i(0)|I_j^i(k)}(x_i^+(0)), \tag{47}$$

where

$$\begin{aligned}
& e'_{\theta_i(0)|I_j^i(k)}(x_i^+(0)) \\
&= \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} \int_{y-\epsilon}^{y+\epsilon} \oint_{\Theta_{\theta'_i(1)|I_j^i(1)}} \cdots \oint_{\Theta_{\theta'_i(k)|I_j^i(k)}} \\
& \quad f_{\theta_i(1), \dots, \theta_i(k)}(z_k, \dots, z_1) f_{\theta_i(0)|\theta_i(k)=z_k, \dots, \theta_i(1)=z_1}(z_0) \\
& \quad \mathbf{d}z_k \cdots \mathbf{d}z_1 \mathbf{d}z_0, \tag{48}
\end{aligned}$$

$\Theta_{\theta'_i(k)|I_j^i(k)}$ is the set of all possible values of $\theta'_i(0)$ under $I_j^i(k)$. Specifically, if $\Theta_{\theta'_i(\ell)|I_j^i(\ell)} \supseteq \Theta_i$ holds for $\ell = 1, \dots, k$, $e'_{\theta_i(0)|I_j^i(k)}(x_i^+(0)) = e_{\theta_i(0)}(x_i^+(0))$ and $\hat{x}_i^*(k) = \hat{x}_i^*(0)$.

Proof: Similar to the proof of Corollary 4.3, if $N_i \not\subseteq N_j$ for $\forall j \in N_i$, there always exists unknown variables in the calculation of $\theta'_i(1), \dots, \theta'_i(k)$. Hence, under $I_j^i(k)$, in (42), $\theta'_i(1), \dots, \theta'_i(k)$ cannot be fixed as constants during the estimation. Taking all the possible values of $\theta'_i(1), \dots, \theta'_i(k)$ into consideration for the estimation, (42) is written as (48).

When $\Theta_{\theta'_i(\ell)|I_j^i(\ell)} \supseteq \Theta_\ell$ holds for $\ell = 1, \dots, k$, we have the following equation

$$\begin{aligned}
& \oint_{\Theta_{\theta'_i(1)|I_j^i(1)}} \cdots \oint_{\Theta_{\theta'_i(k)|I_j^i(k)}} f_{\theta_i(1), \dots, \theta_i(k)|\theta_i(0)} \\
& \quad (z_k, \dots, z_1 | \theta_i(0) = z_0) \mathbf{d}z_k \cdots \mathbf{d}z_1 \\
&= \oint_{\Theta_1} \cdots \oint_{\Theta_k} f_{\theta_i(1), \dots, \theta_i(k)|\theta_i(0)} \\
& \quad (z_k, \dots, z_1 | \theta_i(0) = z_0) \mathbf{d}z_k \cdots \mathbf{d}z_1 \equiv 1,
\end{aligned} \tag{49}$$

holds for $\forall z_0$. It follows that

$$\begin{aligned}
& \int_{y-\epsilon}^{y+\epsilon} \oint_{\Theta_{\theta'_i(1)|I_j^i(1)}} \cdots \oint_{\Theta_{\theta'_i(k)|I_j^i(k)}} f_{\theta_i(1), \dots, \theta_i(k)}(z_k, \dots, z_1) \\
& \quad f_{\theta_i(0)|\theta_i(k)=z_k, \dots, \theta_i(1)=z_1}(z_0) \mathbf{d}z_k \cdots \mathbf{d}z_1 \mathbf{d}z_0 \\
&= \int_{y-\epsilon}^{y+\epsilon} \oint_{\Theta_{\theta'_i(1)|I_j^i(1)}} \cdots \oint_{\Theta_{\theta'_i(k)|I_j^i(k)}} f_{\theta_i(0)}(z_0) \\
& \quad f_{\theta_i(1), \dots, \theta_i(k)|\theta_i(0)}(z_k, \dots, z_1 | \theta_i(0) = z_0) \mathbf{d}z_k \cdots \mathbf{d}z_1 \mathbf{d}z_0 \\
&= \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)}(z_0) \mathbf{d}z_0.
\end{aligned} \tag{50}$$

Thus, (48) is equivalent to

$$\begin{aligned}
e'_{\theta_i(0)|I_j^i(k)}(x_i^+(0)) &= \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} \int_{y-\epsilon}^{y+\epsilon} f_{\theta_i(0)}(z_0) \mathbf{d}z_0 \\
&= e'_{\theta_i(0)}(x_i^+(0)),
\end{aligned} \tag{51}$$

which completes the proof. ■

Note that if all the information used in (2) is available to node j for estimation, then values of $\theta'_i(1), \dots, \theta'_i(k)$ are fixed and known to node j . From Theorem 4.5, we obtain the following corollary directly.

Corollary 4.8: Considering the distributed algorithm (2), if $N_i \subseteq N_j$ and N_i is known to node j , under $I_j^i(k)$, then the optimal distributed estimation of $x_i(0)$ satisfies (41) with

$$\begin{aligned}
e_{\theta_i(0)|I_j^i(k)}(x_i^+(0)) &= \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} \int_{y-\epsilon}^{y+\epsilon} \\
& \quad f_{\theta_i(0)|\theta_i(1)=\theta'_i(1), \dots, \theta_i(k)=\theta'_i(k)}(z) \mathbf{d}z.
\end{aligned}$$

The above three corollaries are correspondingly similar to Corollaries 4.2 to 4.4, respectively.

C. Disclosure Probability under $I_j^i(k)$

The information set that can ensure an accurate estimation is defined by

$$\mathcal{S}_i(k) = \{I_j^i(k) \mid |e_{\theta_i(0)|I_j^i(k)}(x_i^+(0)) - \theta_i(0)| \leq \epsilon\}. \quad (52)$$

Then, define $\mathcal{S}_i^1(k)$ be the set of the first element in $\mathcal{S}_i(k)$, i.e., all the possible $x_i^+(0)$ included in $\mathcal{S}_i(k)$.

$$\mathcal{S}_i^0(k) = \{\theta_i(0) \mid x_i^+(0) \in \mathcal{S}_i^1(k)\}. \quad (53)$$

Clearly, we have $\mathcal{S}_i^1(k) = x_i(0) + \mathcal{S}_i^0(k)$

The following theorem provides an upper bounded of the disclosure probability under $I_j^i(k)$, which is denoted by $\delta(k)$.

Theorem 4.9: Considering the distributed algorithm (2), the disclosure probability δ at iteration k satisfies

$$\delta(k) \leq \oint_{\mathcal{S}_i^0(k)} f_{\theta_i(0)}(z) dz. \quad (54)$$

Proof: Given an $I_j^i(k)$, the optimal distributed estimation $\hat{x}_i^*(k)$ satisfies (41). Then,

$$\begin{aligned} |\hat{x}_i^*(k) - x_i(0)| &\leq \epsilon \\ \Leftrightarrow |x_i^+(0) - x_i(0) - e_{\theta_i(0)|I_j^i(k)}(x_i^+(0))| &\leq \epsilon \\ \Leftrightarrow |\theta_i(0) - e_{\theta_i(0)|I_j^i(k)}(x_i^+(0))| &\leq \epsilon. \end{aligned} \quad (55)$$

From the definition of δ , we have

$$\begin{aligned} \delta(k) &= \Pr\{|\hat{x}_i^*(k) - x_i(0)| \leq \epsilon\} \\ &= \Pr\{|\theta_i(0) - e_{\theta_i(0)|I_j^i(k)}(x_i^+(0))| \leq \epsilon\} \\ &= \oint_{\mathcal{S}_i(k)} f_{I_j^i(k)}(z) dz, \end{aligned} \quad (56)$$

where $f_{I_j^i(k)}(z)$ is the PDF of $I_j^i(k)$ (since $I_j^i(k)$ is random under the distributed algorithm). From the above function, it is hard to calculate the value of δ , since $f_{I_j^i(k)}(z)$ is unknown and difficult to obtain due to the coupled input random variables. However, note that for each $I_j^i(k) \in \mathcal{S}_i(k)$,

its element $x_i^+(0)$ should satisfy $x_i^+(0) - x_i(0) = \theta_i(0)$ and $\theta_i(0) \in \mathcal{S}_i^0(k)$. It means that only if $\theta_i(0) \in \mathcal{S}_i^0(k)$, $|\theta_i(0) - e_{\theta_i(0)|I_j^i(k)}(x_i^+(0))| \leq \epsilon$ can be true. Thus,

$$\begin{aligned} \delta(k) &= \oint_{\mathcal{S}_i(k)} f_{I_j^i(k)}(z) dz \\ &\leq \oint_{\mathcal{S}_i^0(k)} f_{\theta_i(0)}(z) dz, \end{aligned} \quad (57)$$

which completes the proof. \blacksquare

If there exist other conditions for estimation, e.g., independent noise inputs, we obtain the closed-form expression of δ , and thus we have the following theorem.

Theorem 4.10: Considering the distributed algorithm (2), under $I_j^i(k)$, if one of the following conditions holds,

- 1) the added noise sequence $\theta_i(0), \dots, \theta_i(k)$ are independent of each other;
- 2) $\Theta_{\theta_i(\ell)|I_j^i(\ell)} \supseteq \Theta_i$ or $\Theta_{\theta_i(\ell)|I_j^i(\ell)} = \mathcal{R}$ holds for $\ell = 1, \dots, k$ and $\forall k \geq 1$;

then $\delta(k) = \delta$ holds for $\forall k \geq 0$ and δ satisfies (19). Furthermore, if $\mathcal{X}_i = \mathcal{R}$, δ satisfies (20).

The above theorem can be obtained from Corollaries 4.6 and 4.7 and Theorem 3.3, so we omit its proof.

D. Calculation of the Optimal Estimation

From the discussions in the above subsections, the optimal distributed estimation of $x_i(0)$ is the most important factor for the privacy analysis. We design an algorithm to calculate the optimal distributed estimation of $x_i(0)$ under $I_j^i(k)$ for $\forall k \geq 0$. From Theorem 4.5, one infers that the key challenge to obtain $\hat{x}_i^*(k)$ is to calculate $e_{\theta_i(0)|I_j^i(k)}(x_i^+(0))$. Similar to the general approach given in Sec. III-A, we design Algorithm 1 to calculate $e_{\theta_i(0)|I_j^i(k)}(x_i^+(0))$.

V. CASE STUDIES AND OPTIMAL NOISES

Privacy-preserving average consensus algorithm (PACA) is a typical privacy-preserving distributed algorithm, which aims to guarantee that the privacy of the initial state is preserved and at the same time the average consensus can still be achieved [15], [17], [19]. The basic idea of PACA is adding and subtracting variance decaying and zero-sum random noises to the traditional consensus process. Differential privacy of PACA has been studied in [17]. In this section, we focus on data privacy analysis of PACA. We adopt the developed theories in the above section

Algorithm 1 : Calculation of $e_{\theta_i(0)|I_j^i(k)}(x_i^+(0))$

1: **Input:** the information $I_j^i(k)$, the PDFs $f_{\theta_i(0)}(z), \dots, f_{\theta_i(k)}$.

2: **Calculation:** Using the correlation among $\theta_i(0), \dots, \theta_i(k)$ to obtain joint PDF $f_{\theta_i(1), \dots, \theta_i(k)}(\theta'_i(1), \dots, \theta'_i(k))$ and the conditional PDF $f_{\theta_i(0)|\theta_i(k)=\theta'_i(k), \dots, \theta_i(1)=\theta'_i(1)}$.

3: Computing the following derivative to obtain $f'_\theta(y, \epsilon)$,

$$\frac{\partial \int_{y-\epsilon}^{y+\epsilon} f'_\theta(z) dz}{\partial y} = F'_\theta(y, \epsilon) \quad (58)$$

where

$$\begin{aligned} f'_\theta(z) &= f_{\theta_i(1), \dots, \theta_i(k)}(\theta'_i(1), \dots, \theta'_i(k)) \\ f_{\theta_i(0)|\theta_i(k)=\theta'_i(k), \dots, \theta_i(1)=\theta'_i(1)}(z) & \end{aligned} \quad (59)$$

4: Solving the following equation to obtain the zero point set, $\Omega_{F'_\theta}^0$,

$$F'_\theta(y, \epsilon) = 0. \quad (60)$$

5: Calculating the set of

$$\mathcal{X}_{x_i^+(0)} = \{x_i^+(0) - \mathcal{X}_i\} \cap \Omega_{f'_\theta}^0 \cup \{x_i^+(0) - \mathcal{X}_i\}_b.$$

6: Obtaining the estimation by

$$e_{\theta_i(0)|I_j^i(k)}(x_i^+(0)) = \arg \max_{y \in \mathcal{X}_{x_i^+(0)}} \int_{y-\epsilon}^{y+\epsilon} f'_\theta(z) dz. \quad (61)$$

7: **Output:** the estimation of $e_{\theta_i(0)|I_j^i(k)}(x_i^+(0))$.

to analyze the (ϵ, δ) -data-privacy of the PACA algorithm, and then find the optimal noises for the algorithm to achieve the highest data privacy.

A. Privacy of PACA

Referring to the existing algorithms, we describe the PACA algorithm as follows:

$$\begin{aligned} x_i(k+1) &= f_i(x_i^+(k), x_j^+(k) : j \in N_i) \\ &= w_{ii}(x_i(k) + \theta_i(k)) + \sum_{j \in N_i} w_{ij}(x_j(k) + \theta_j(k)), \end{aligned} \quad (62)$$

for $\forall i \in V$ and $k \geq 0$, where w_{ii} and w_{ij} are weights, and its matrix form is given by

$$x(k+1) = W(x(k) + \theta(k)), k \geq 0, \quad (63)$$

where $W \geq 0 \in \mathcal{R}^{n \times n}$ is a doubly stochastic matrix satisfying $w_{ii} > 0$ and $w_{ij} > 0$ for $(i, j) \in E$; and each $\theta_i(k) \in \theta(k)$ satisfies $\mathbf{Var}\{\theta_i(k)\} < \rho \mathbf{Var}\{\theta_i(k-1)\}$ (where $0 < \rho < 1$) and $\sum_{k=0}^{\infty} \theta_i(k) = 0$. When $\theta(k) = 0$ for $k \geq 0$, it is proved in [24] that an average consensus is achieved by (63), i.e.,

$$\lim_{k \rightarrow \infty} x(k) = \frac{\sum_{\ell=1}^n x_{\ell}(0)}{n} \mathbf{1} = \bar{x}. \quad (64)$$

When $\theta(k) \neq 0$ for $k \geq 0$, it is proved in [19] that an average consensus is achieved by (63) in the mean-square sense.

The following two theorems analyze the data privacy of the PACA algorithm under the conditions that node j can and cannot have all the information used in the iteration process for the estimation, respectively.

Theorem 5.1: If $N_i \subseteq N_j$ and N_i is known to node j for $j \in N_i$, using PACA, we have $\delta = 1$ holds for $\forall \epsilon > 0$, i.e., $x_i(0)$ is perfectly inferred.

Proof: When $N_i \subseteq N_j$ and N_i is known to node j for $j \in N_i$, then the values of $\theta'_i(1), \dots, \theta'_i(\infty)$ are fixed and released to node j under $I_j^i(\infty)$. From Corollary 4.8, it follows that

$$\begin{aligned} e_{\theta_i(0)|I_j^i(\infty)}(x_i^+(0)) &= \arg \max_{y \in \{x_i^+(0) - \mathcal{X}_i\}} \int_{y-\epsilon}^{y+\epsilon} \\ &\quad f_{\theta_i(0)|\theta_i(1)=\theta'_i(1), \dots, \theta_i(\infty)=\theta'_i(\infty)}(z) \mathbf{d}z. \end{aligned} \quad (65)$$

Meanwhile, from $\sum_{k=0}^{\infty} \theta_i(k) = 0$, it follows that $\theta_i(0) = -\sum_{k=1}^{\infty} \theta_i(k)$. Hence, in the right side of (65), the maximum value of the integral is achieved when $y = -\sum_{k=1}^{\infty} \theta_i(k)$, i.e.,

$$e_{\theta_i(0)|I_j^i(\infty)}(x_i^+(0)) = -\sum_{k=1}^{\infty} \theta'_i(k) = \theta_i(0).$$

Then, we have

$$\begin{aligned}\hat{x}_i^*(\infty) &= x_i^+(0) - e_{\theta_i(0)|I_j^i(\infty)}(x_i^+(0)) \\ &= x_i^+(0) - \theta_i(0) = x_i(0),\end{aligned}$$

i.e., $x_i(0)$ is perfectly inferred, and thus $\delta = 1$. ■

In the above proof, Corollary 4.8 is adopted to prove the theorem. Actually, if $\theta'_i(1), \dots, \theta'_i(\infty)$ are fixed and released, the values of $\theta_i(1), \dots, \theta_i(\infty)$ are released to node j . Then, using the condition $\sum_{k=0}^{\infty} \theta_i(k) = 0$, we can obtain $\theta_i(0)$, and thus $x_i(0)$ is obtained from using $x_i^+(0) - \theta_i(0) = x_i(0)$. It obtains the same results as Theorem 5.1, and thus verifies the results of Corollary 4.8.

Theorem 5.2: If $N_i \not\subseteq N_j$ for $\forall j \in N_i$ and $\Theta_i(k) = \mathcal{R}$ for $\forall i \in V$, then the PACA algorithm achieves (ϵ, δ) -data-privacy, where δ satisfies (19), and then if $\mathcal{X}_i = \mathcal{R}$, δ satisfies (20).

Proof: Since the conclusion in this theorem are the same as Theorem 4.10, we prove it by showing that one of the conditions in Theorem 4.10 holds. Since $N_i \not\subseteq N_j$ for $\forall j \in N_i$, which means that any neighbor node j cannot obtain all the information using in the right-hand side of (62) at each iteration k . Hence, there exists at least one $x_{j_0}^+(k-1)$ ($j_0 \neq j$ and $j_0 \in N_i$) which is not available to node j for estimation. Note that under the PACA algorithm,

$$\theta'_i(k) = x_i^+(k) - (w_{ii}x_i^+(k-1) + \sum_{j \in N_i} w_{ij}x_j^+(k-1)).$$

Since $x_{j_0}^+(k-1) = x_{j_0}(k-1) + \theta_{j_0}(k-1)$ and $\theta_{j_0}(k-1) \in \Theta_{j_0}(k-1) = \mathcal{R}$, we have $\theta'_i(k) \in \mathcal{R}$ during the estimation, i.e., $\Theta_{\theta'_i(k)|I_j^i(k)} = \mathcal{R}$. Therefore, the second condition in Theorem 4.10 holds, and we thus have completed the proof. ■

With the above theorem, it is not difficult to prove that the algorithms proposed in both [19] and [6] provide (ϵ, δ) -data-privacy and δ satisfies (20).

B. Optimal Noises

In this subsection, we consider the optimization problem (8). It is known that the noise adding process given in PACA can ensure that the average consensus can be achieved by the algorithm, which means that the constraint in (8) is satisfied. Meanwhile, from Theorem 5.2, it follows that δ satisfies (19), when node j cannot know all the information using in the consensus process at

each iteration. Thus, under PACA, problem (8) is equivalent to an unconstrained minimization problem as follows,

$$\min_{f_{\theta_i(0)}(y)} \delta = \oint_{\mathcal{S}_i(0)} f_{\theta_i(0)}(y) dy. \quad (66)$$

In problem (66), there is no constraint on $f_{\theta_i(0)}(y)$ and it can be a PDF of any distribution of noises. Hence, we can find a $f_{\theta_i(0)}(y)$ with a large variance such that δ is smaller than any given small value since $\mathcal{S}_i(0)$ is a bounded set. For example, when $\mathcal{X}_i = \mathcal{R}$, we have $\mathcal{S}_i(0) = [e_{\theta_i(0)} - \epsilon, e_{\theta_i(0)} + \epsilon]$. Then, a uniform distribution with $f_{\theta_i(0)}(y) \leq \frac{1}{M}$ (M is a constant) can ensure that

$$\delta = \oint_{\mathcal{S}_i(0)} f_{\theta_i(0)}(y) dy \leq \frac{2\epsilon}{M}. \quad (67)$$

which means that δ can be an arbitrarily small value as M can be set arbitrarily large. Hence, one concludes that, by adding uniformly distributed noises, PACA can provide (ϵ, δ) -data-privacy with any small δ .

Then, we consider the case that the variance of $\theta_i(0)$ is a constant. Note that a smaller ϵ means a higher accuracy estimation. It means that when ϵ becomes smaller, the value of δ is more important for the privacy preservation. Hence, we define the optimal distribution in the sense of the data-privacy as follows.

Definition 5.3: We say $f_{\theta_i(0)}^*(y)$ is the optimal distribution of $\theta_i(0)$ for a PACA. If, for any given distribution $f_{\theta_i(0)}^1(y)$, there exists an ϵ_1 such that $\delta(f_{\theta_i(0)}^*(y), \epsilon) < \delta(f_{\theta_i(0)}^1(y), \epsilon)$ holds for $\forall \epsilon \in (0, \epsilon_1]$.

Based on Definition 5.3, we formulate the following minimization problem,

$$\begin{aligned} \min_{f_{\theta_i(0)}(y)} \quad & \delta, \\ \text{s.t.} \quad & \mathbf{Var}\{\theta_i(0)\} = \sigma^2. \end{aligned} \quad (68)$$

From our previous research on this optimization problem [25], the optimal solution is that the noise $\theta_i(0)$ should follow a uniform distribution given $\epsilon \leq \sigma$.

VI. CONCLUSIONS

In this paper, we have investigated the optimal distributed estimation and privacy problem for privacy-preserving distributed algorithm. We introduced the definition of the optimal distributed

estimation and the (ϵ, δ) -data-privacy definition, which reveals the relationship between the privacy and the estimation accuracy. A theoretical framework was provided for the optimal distributed estimation and the privacy analysis, where both the closed-form expressions of the optimal distributed estimation and the privacy parameters were obtained. With the obtained framework, we proved that the existing PACA algorithm is (ϵ, δ) -data-private and the optimal noises, which guarantees the minimized disclosure probability, was obtained. The applications of the proposed framework will be considered in our future work.

REFERENCES

- [1] S. Kar and J. M. Moura. "Asymptotically efficient distributed estimation with exponential family statistics," *IEEE Trans. on Information Theory*, 60(8): 4811–4831, 2014.
- [2] A. Nedic, and A. Olshevsky. "Distributed optimization over time-varying directed graphs," *IEEE Trans. on Automatic Control*, 60(3): 601-615, 2015.
- [3] M. Andreasson, D. Dimarogonas, H. Sandberg, and K. H. Johansson. "Distributed control of networked dynamical systems: Static feedback, integral action and consensus," *IEEE Trans. on Automatic Control*, 59(7): 1750-1764, 2014.
- [4] V. Gulisano, V. Tudor, M. Almgren, and M. Papatriantafilou. "BES: Differentially private and distributed event aggregation in advanced metering infrastructures," in *Proc. of ACM IWCPSS*, 2016.
- [5] Z. Huang, S. Mitra, and N. Vaidya. "Differentially private distributed optimization," in *Proc. of ACM ICDCN*, 2015.
- [6] J. He, L. Cai, P. Cheng, M. Xing, J. Pan and L. Shi. Private and accurate data aggregation against dishonest nodes. <https://arxiv.org/pdf/1609.06381v2.pdf>, 2016.
- [7] 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.
- [8] F. Pasqualetti, R. Carli, A. Bicchi, and F. Bullo. "Distributed estimation and detection under local information," in *Proc. of IFAC*, 2010.
- [9] G. Mateos, I. Schizas and G. Giannakis. "Distributed recursive least-squares for consensus-based in-network adaptive estimation," *IEEE Trans. Signal Processing*, 57(11): 4583–4588, 2009.
- [10] 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*, DOI: 10.1109/TSG.2015.2513772.
- [11] 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.
- [12] L. Schenato and F. Fiorentin. "Average timesynch: A consensus-based protocol for clock synchronization in wireless sensor networks," *Automatica*, 47(9): 1878–1886, 2011.
- [13] 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.
- [14] 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.
- [15] J. Le Ny and G. Pappas. "Differentially private filtering," *IEEE Trans Automat. Contr.*, 59(2): 341–354, 2014.

- [16] Z. Huang, S. Mitra, and G. Dullerud. “Differentially private iterative synchronous consensus.” in *Proc. ACM Workshop on Privacy in the Electronic Society*, 2012.
- [17] E. Nozari, P. Tallapragada, and J. Cortes. “Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design.” *arXiv preprint arXiv:1512.09039*, 2016.
- [18] N. Maniara and C. Hadjicostis. “Privacy-preserving asymptotic average consensus.” in *Proc. IEEE ECC*, 2013.
- [19] Y. Mo, and R. Murray. “Privacy preserving average consensus,” *IEEE Trans. Automat Contr.*, 62(2): 753–765, 2017.
- [20] C. Dwork. “Differential privacy,” in *Automata, languages and programming*, Springer, 1-12, 2006.
- [21] Q. Geng and P. Viswanath. “The optimal noise-adding mechanism in differential privacy,” *IEEE Trans. on Information Theory*, 62(2): 925-951, 2016.
- [22] Q. Geng and P. Viswanath. “Optimal noise adding mechanisms for approximate differential privacy,” *IEEE Trans. on Information Theory*, 62(2): 952-969, 2016.
- [23] J. He and L. Cai. Differential private noise adding mechanism: Conditions and its application on consensus. <https://arxiv.org/abs/1611.08936>, 2016.
- [24] A. Olshevsky and J. Tsitsiklis. “Convergence speed in distributed consensus and averaging,” *SIAM Review*, 53(4): 747–772, 2011.
- [25] J. He, L. Cai, C. Zhao, P. Cheng, and X. Guan. Privacy-preserving average consensus: privacy analysis and optimal algorithm design. <https://arxiv.org/pdf/1609.06368.pdf>, 2017.
- [26] H. Kargupta, S. Datta, Q. Wang, and K. Sivakumar. On the privacy preserving properties of random data perturbation techniques. In *Proc. IEEE ICDM*, 2003.