Preprints of the 21st IFAC World Congress (Virtual)
Berlin, Germany, July 12-17, 2020

Dynamic Privacy-preserving Collaborative Schemes for Average Computation

Xin Wang * **Hideaki Ishii** ** **Jianping He** *** **Peng Cheng** *

* *State Key Lab. of Industrial Control Technology, Zhejiang University, Hangzhou, 310027, China. Emails: xinw.zju@gmail.com; pcheng@iipc.zju.edu.cn*
** *Dept. of Computer Science, Tokyo Institute of Technology, Yokohama, 226-8502, Japan. Email: ishii@c.titech.ac.jp*
*** *Dept. of Automation, Shanghai Jiao Tong University, Shanghai, 200240, China. Email: jphe@sjtu.edu.cn*

Abstract: In this paper, we consider the privacy-preserving problem in collaborative computing. Based on a two-step average computation framework, we propose three privacy-aware schemes, all of which achieve different levels of privacy protections depending on data servers' trust degrees. Further, by carefully designing noises injected to the distributed computing process, we obtain dynamic privacy-preserving schemes, whose privacy preserving levels are measured by Kullback-Leibler differential privacy. In addition, we prove that the proposed schemes achieve convergence in different senses. Numerical experiments are finally conducted to verify the obtained privacy properties and convergence guarantees.

Keywords: Collaborative computing, dynamic privacy, average consensus, convergence.

1. INTRODUCTION

With the popularity of smart devices, zettabytes of data is generated by people, machines and things every day (Cisco (2018)). To efficiently deal with such large-scale data, collaborative computing (Smith et al. (2017)) has been proposed by using the computation and communication resources of multiple servers (or clusters). However, when the generated data is related to people's daily lives, e.g., medical records (Fredrikson et al. (2014)), power consumption (Asghar et al. (2017)) and social relationships (Qin et al. (2017)), privacy has to be attached significant attention during the conduction of computation tasks.

One reasonable idea to mitigate privacy disclosure is to assign some protection control rights to data contributors (DCs), as claimed by Wang et al. (2019b). In this case, even when the data servers (DSs) are completely compromised by adversaries, the disclosed data is the version under privacy processing by DCs. On the other hand, in collaborative computing, different DSs are given diverse trust degrees by a DC. Considering the locations and network authorities, a DC usually reports his/her data to a DS (or DS cluster) and views that DS as a more trustworthy party. On the contrary, other DSs having no direct connection with him/her are given lower trust degrees. It is required by the setting of diverse trust degrees that the communicated information about DCs' data should provide stronger privacy guarantee when DSs collaboratively execute a computation task through interactions.

⋆ This work was partially supported by the NSFC under Grant 61761136012, 61533015 and 61973218, the JST CREST Grant No. JPMJCR15K3, and JSPS under Grant-in-Aid for Scientific Research Grant No. 18H01460. The support provided by China Scholarship Council (No. 201806320306) is also acknowledged.

In the literature, a series of privacy-aware schemes have been proposed for distributed algorithms in recent years. For the computation of average value of DCs' data, noise obfuscation based preservation approaches can be found in Huang et al. (2012), Mo and Murray (2017), Nozari et al. (2017) and He et al. (2019). In particular, the schemes in Huang et al. (2012) and Nozari et al. (2017) were proved to be differentially private, which is one of the current data privacy standards (Dwork (2008)). Similarly, through carefully-designed noise injection, Duan et al. (2015) and Wang et al. (2019a) proposed privacy-preserving maximum consensus mechanisms, and the privacy-aware distributed optimization schemes can be found in Hsieh et al. (2017) and Gade and Vaidya (2018). In addition, by utilizing homomorphic encryption methods, Ruan et al. (2019) achieves average consensus under untrustworthy servers setting. However, in these works, DCs report their original data to DSs, causing that the privacy protection is controlled by only DSs. Moreover, there exists an assumption that all the participating DSs have the same trust degrees. Under this assumption, the requirement for different levels of privacy protections may not be satisfied with these existing schemes.

In this paper, we consider a heterogeneous privacy-preserving problem in collaborative computing by following the framework first proposed by Wang et al. (2019b); this approach was further extended to distributed classification problems in (Wang et al. (2019c)). Here, we focus on the effects brought by dynamic characteristics of the distributed algorithm for privacy protection. This aspect was not analyzed before since Wang et al. (2019b) gave only an upper bound of the privacy loss when the algorithm converges. Since most existing distributed algorithms run in

an iterative manner (Bullo (2019)), the information about DC's sensitive data is released in each iteration. Thus, it is critical to study novel privacy-aware schemes, where the privacy loss changes dynamically as iterative release of private information. This problem will be referred to as the dynamic privacy-preserving collaborative computing problem. Particularly, how to guarantee the privacy loss in each iteration to be controllable and quantifiable is the most challenging issue in the problem.

In particular, based on the two-step computation framework proposed by Wang et al. (2019b), we further design different noise-injection based approaches for the distributed average computing process. By employing Kullback-Leibler differential privacy (KLDP) (Cuff and Yu (2016)), we analyze the dynamic privacy properties of the proposed schemes, and give their privacy preserving levels (PPLs) in different iterations. In addition, the convergence performance analysis about these privacy-aware schemes is established. We find that there exists a tradeoff between privacy preservation and convergence guarantee.

The main contributions of this paper are threefold: i) We propose three privacy-preserving schemes, which achieve different privacy protections and convergence guarantees; ii) we prove that all the proposed schemes preserve KLDP, and derive their theoretical PPLs; iii) we further prove that the three schemes achieve convergence in distinct senses with respect to the average value of all DCs' reported data.

The remainder of this paper is organized as follows. Section 2 formulates the considered problem. Section 3 presents the main results, and the performance evaluation is shown in Section 4. Finally, Section 5 concludes the paper.

2. PROBLEM FORMULATION

2.1 Computation framework

We use the two-step collaborative computing framework to compute the average value of large-scale data, which is first proposed by Wang et al. (2019b). Two parties participate in the framework: Data contributors (DCs) and data servers (DSs). The main workflow is that DSs first collect data from different DCs and then compute their average value in a fully distributed way, which is denoted by Step 1 and Step 2, respectively.

Network Model. An undirected and connected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is used to describe the interaction network between DSs, where $\mathcal{V}$ is the set of $n \geq 2$ DSs and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ denotes the set of edges linking different DSs. An edge $(i, l) \in \mathcal{E}$ implies that DSs i and l can communicate with each other. For a DS $i \in \mathcal{V}$, the set of its neighbor DSs is denoted by $\mathcal{N}_i$, i.e., $\mathcal{N}_i = \{l \in \mathcal{V} \mid (i, l) \in \mathcal{E}\}$.

All DCs are partitioned into n disjoint groups in terms of their locations, and the data of each group is collected by a DS. Denote the group of DCs reporting data to DS i as $\mathcal{U}_i$, and $m_i = |\mathcal{U}_i|$ is the number of such DCs. We consider that DC $j \in \mathcal{U}_i, \forall i, j$, has private data $x_{i,j} \in \mathbb{R}$. The average value of all DCs' data is

$$\overline{x} = \frac{1}{\sum_{i=1}^{n} m_i} \sum_{i=1}^{n} \sum_{j=1}^{m_i} x_{i,j}. \tag{1}$$

Then, we introduce how to use the framework to compute the average value.

First, in Step 1, all DCs report their private data to corresponding DSs. Suppose that the end time of Step 1 is $t = T_0$, which is also the beginning time of Step 2. We denote the state of DS i at time t as $y_i(t)$. At time T_0, DS i aggregates the received data and sets its initial state as

$$y_i(T_0) = \frac{n}{\sum_{i=1}^{n} m_i} \sum_{j=1}^{m_i} x_{i,j}.$$

Next, all DSs compute the average value iteratively by communicating their collected data. An average consensus algorithm is used to update the states of DSs. At time $t > T_0$, DS i computes its state as

$$y_i(t+1) = w_{ii} y_i(t) + \sum_{l \in \mathcal{N}_i} w_{il} y_l(t), \tag{2}$$

where w_{ii} and w_{il} are the weights. Here, we adopt the Metropolis weights (Xiao et al. (2005)) defined as

$$w_{il} = \begin{cases} \dfrac{1}{1 + \max\{|\mathcal{N}_i|, |\mathcal{N}_l|\}}, & \text{if } (i,l) \in \mathcal{E}, \\ 1 - \displaystyle\sum_{k \in \mathcal{N}_i} w_{ik}, & \text{if } i = l, \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

It is proved by Xiao et al. (2005) that under the weights in (3), the states of all DSs asymptotically converge to the average value in (1), i.e., $\lim_{t \to \infty} y_i(t) = \overline{x}, \forall i \in \mathcal{V}$.

2.2 Privacy-preserving issue

We consider that DCs' data $x_{i,j}, \forall i, j$, is privacy-sensitive, whose original value should not be disclosed to any DSs. Here, all DSs are untrustworthy, but different DSs are given diverse trust degrees by each DC. Specifically, for a DC $j \in \mathcal{U}_i$, the DSs are divided into two categories of potential privacy eavesdroppers: DS i is the first category while other DSs $l \in \mathcal{V}, l \neq i$, are the second type. The first type is given higher trust degrees than the second type. This implies that a DC's information disclosed to the second type should provide stronger protection.

Privacy metric. To measure the privacy guarantee, we use the Kullback-Leibler differential privacy (KLDP) proposed by Cuff and Yu (2016). We define a privacy-preserving mechanism $M : \mathbb{R}^d \to \mathbb{R}$, which takes a private vector $\mathbf{q} \in \mathbb{R}^d$ with any dimension $d \geq 1$ as input and outputs a randomized message about $\mathbf{q}$. For two inputs, KLDP describes the similarity between the distributions of their outputs under M. Obviously, the higher the similarity, the more difficult it is for the eavesdropper to identify the difference in the inputs. Now, we give the formal definition of KLDP. In the definition, we use $D_{KL}(\cdot\|\cdot)$ to denote the Kullback-Leibler divergence. For two distributions P and S, we define their Kullback-Leibler divergence as

$$D_{KL}(P\|S) = \int_{-\infty}^{\infty} p(z) \log \frac{p(z)}{s(z)} dz,$$

where $p(z)$ and $s(z)$ are the probability density functions (PDFs) of P and S, respectively.

***Definition** 1.* (ϵ-KLDP). Given a scalar $\epsilon > 0$, a privacy-preserving mechanism M preserves ϵ-KLDP if for any two

vectors $\mathbf{q}, \mathbf{q}' \in \mathbb{R}^d$ satisfying with $k_0 \in \{1, 2, \cdots, d\}$ and $\alpha > 0$, $|q_{k_0} - q'_{k_0}| \leq \alpha$ and $|q_k - q'_k| = 0, \forall k \neq k_0$, it holds

$$\frac{D_{KL}\left[P_{M(\mathbf{q})} \| P_{M(\mathbf{q}')}\right] + D_{KL}\left[P_{M(\mathbf{q}')} \| P_{M(\mathbf{q})}\right]}{2} \leq \epsilon, \quad (4)$$

where $P_{M(\cdot)}$ is the distribution of $M(\cdot)$.

In Definition 1, ϵ denotes the privacy-preserving level (PPL). A smaller ϵ indicates higher similarity between $P_{M(\mathbf{q})}$ and $P_{M(\mathbf{q}')}$, that is, stronger privacy protection. The difference between the two similar inputs is described by parameter α, called the adjacent distance. The objective of introducing M is to guarantee that the adjacent distance is reflected in the outputs as little as possible. It is more difficult to obfuscate the effect of α when it is larger. Specifically, for two adjacent distances α_1 and α_2 satisfying $\alpha_1 \geq \alpha_2$, if the same PPL is required, then M should introduce more uncertainties for α_1.

Private information inference. When the DSs receive information about DCs' private data, they will make inference by the help of side information. For the first type of privacy eavesdroppers, the data reported by DCs in Step 1 is directly leveraged for inference. The DSs in the second type conduct privacy inference by mainly utilizing the information communicated with other DSs. In addition, various side information will be combined to assist the inference. We have the following assumption.

Assumption 1. The weights $w_{il}, \forall l$ in (2) are known to DS i's neighbors. At time t, the information set $\mathcal{I}_i(t) = \{y_l(t) \mid l \in \mathcal{N}_i \bigcup \{i\}\}$ is available for other DSs to make privacy inference.

2.3 Problem setup

In this paper, we will propose novel privacy-preserving schemes, which further achieve dynamic privacy guarantee in Step 2 on the basis of heterogeneous protections. Since all DSs are untrustworthy, in Step 1, DCs first obfuscate the original data in their local devices as

$$\widetilde{x}_{i,j} = x_{i,j} + \eta_{i,j}, j \in \mathcal{U}_i, \quad (5)$$

where $\eta_{i,j} \sim \mathcal{N}(0, \sigma_{i,j}^2)$ is a zero-mean Gaussian noise. Then, the noisy version $\widetilde{x}_{i,j}$, instead of $x_{i,j}$, will be reported to DS i. The obfuscation in (5) is also the private mechanism $M_1 : \mathbb{R} \to \mathbb{R}$ used in Step 1. For the property of M_1, we have the following lemma (Wang et al. (2019b)).

Lemma 1. Given $\alpha > 0$, the mechanism M_1 preserves $\frac{\alpha^2}{2\sigma_{i,j}^2}$-KLDP under (5).

In Step 2, to provide stronger privacy guarantee, DSs will further introduce some randomization into the messages before communicating with neighbors. At time $t \geq T_0$, after updating $y_i(t)$ by (2), DS i perturbs $y_i(t)$ as

$$\widetilde{y}_i(t) = y_i(t) + \theta_i(t), \quad (6)$$

where $\theta_i(t)$ is the noise to be designed to meet different privacy requirements. It is noted that $\theta_i(t)$ can be 0, implying no noise perturbation. The perturbed state $\widetilde{y}_i(t)$ will be sent to neighbors and further used for state update. That is, (2) is replaced by

$$y_i(t+1) = w_{ii}\left(y_i(t) + \theta_i(t)\right) + \sum_{l \in \mathcal{N}_i} w_{il}\left(y_l(t) + \theta_l(t)\right). \quad (7)$$

Obviously, the added noises $\theta_i(t), \forall i$, also affect the convergence performance of the framework and the accuracy of the computed average value. Hence, the goal of this paper is to design $\theta_i(t)$, which can satisfy diverse requirements for privacy protection in Step 2 and achieve different convergence guarantees.

3. MAIN RESULTS

In this section, we will design three forms of $\theta_i(t)$, and analyze their corresponding privacy protections and convergence performances.

Before designing $\theta_i(t)$, we first analyze the computed results under the reported noisy data $\widetilde{x}_{i,j}, \forall i, j$. If all DCs obfuscate their private data using (5), then with (2), the computed average value is given by

$$\widehat{x} = \frac{1}{\sum_{i=1}^n m_i} \sum_{i=1}^n \sum_{j=1}^{m_i} \widetilde{x}_{i,j}. \quad (8)$$

For the computation accuracy of $\widehat{x}$, we have the following lemma (Wang et al. (2019b)).

Lemma 2. $\widehat{x}$ is an unbiased estimate of $\overline{x}$, that is, $\mathbb{E}_{\{\eta_{i,j}\}}[\widehat{x}] = \overline{x}$. For $\delta \in (0, 1)$, the distance $|\widehat{x} - \overline{x}|$ satisfies with probability at least $1 - \delta$

$$|\widehat{x} - \overline{x}| \leq \frac{1}{\sum_{i=1}^n m_i} \sqrt{\frac{1}{\delta} \sum_{i=1}^n \sum_{j=1}^{m_i} \sigma_{i,j}^2}. \quad (9)$$

Note that $\widehat{x}$ is computed without perturbation in Step 2. Since the noises $\eta_{i,j}, \forall i, j$, are unknown to DSs, $\theta_i(t)$ added in Step 2 cannot be used to reduce the uncertainty in the reported data. Thus, $\widehat{x}$ can be viewed as the best computed results based on DCs' reported data, and then is used as the reference average value. For the performance analysis in Step 2, we will investigate the relations between the computed results under $\theta_i(t)$-perturbation and $\widehat{x}$.

3.1 Scheme 1: Initial state perturbation

With Assumption 1, we find that the updated states $y_i(t+1), t \geq T_0$, can be inferred, causing the added noise $\theta_i(t+1), t \geq T_0$, to be computed directly. In this case, the extra noises added at time $t \geq T_0 + 1$ are meaningless from the perspective of privacy protection. Thus, we first adopt the idea of initial state perturbation, where only $y_i(T_0)$ is obfuscated by a noise. From (2), we know that when there is no noise perturbation at $t \geq T_0 + 1$, $y_i(t)$ is a linear combination of DSs' initial states. It is noted that linear combination does not change uncertainties of independent random variables. This implies the privacy guarantee in Step 2 is determined by $\widetilde{y}_i(T_0)$ and does not change with iterations. In this paper, we select a zero-mean Gaussian noise $\theta_i(T_0) \sim \mathcal{N}(0, \sigma_i^2)$ to perturb $y_i(T_0)$. Now, we give the form of the noise $\theta_i(t)$ as

$$\theta_i(t) = \begin{cases} \theta_i(T_0), & t = T_0, \\ 0, & \text{otherwise.} \end{cases} \quad (10)$$

Also, (10) can be viewed as the privacy-aware mechanism M_2^1 used in Step 2, where the superscript 1 indicates that the current mechanism is Scheme 1. Different from M_1, the input of M_2^1 is an m_i-dimensional vector aggregating

the data reported by the DCs in $\mathcal{U}_i$. Thus, we have $M_2^1 : \mathbb{R}^{m_i} \to \mathbb{R}$, where the output in each iteration is a scalar $\widetilde{y}_i(t)$. The following theorem gives the privacy-preserving property of M_2^1.

***Theorem** 1.* Given $\alpha > 0$, the mechanism M_2^1 preserves $\frac{\alpha^2}{2\sum_{j=1}^{m_i}\sigma_{i,j}^2+2\left(\sum_{i=1}^{n} m_i/n\right)^2\sigma_i^2}$-KLDP.

It is noted that for DC $j \in \mathcal{U}_i$, the PPL does not decrease in subsequent iterations, and all DCs in $\mathcal{U}_i$ obtain the same privacy guarantee. In addition, the protection will be stronger if DS i makes the perturbation using a noise with larger variance.

Next, we analyze the convergence performance.

***Lemma** 3.* If all DSs use (7) to update states, where the noises $\theta_i(t), \forall i$, are set by (10), then the states of DSs converge to $\widehat{x}$ in the sense of expectation, i.e.,

$$\lim_{t\to\infty} \mathbb{E}_{\{\theta_i(t)\}}\left[\widetilde{y}_i(t) - \widehat{x}\right] = 0, \forall i. \tag{11}$$

3.2 Scheme 2: Zero-sum noises perturbation

From Lemma 3, we know that Scheme 1 only achieves convergence in expectation, which is a relatively weak guarantee. In Scheme 2, we will use multi-iteration noise perturbation to explore a stronger convergence guarantee. To this end, the uncertainty brought by $\theta_i(T_0)$ should be reduced, which simultaneously weakens the privacy protection. Nevertheless, if each iteration brings a controllable degree of privacy decrease and the time when the uncertainty completely vanishes is costly, the protection is also accepted.

In Scheme 2, at time $t \geq T_0$, DS i first generates a zero-mean Gaussian noise $\varphi_i(t) \sim \mathcal{N}(0, \rho^{t-T_0}\sigma_i^2)$, where $0 < \rho < 1$. When $t = T_0$, $y_i(T_0)$ is perturbed by $\varphi_i(T_0)$, that is, $\theta_i(T_0) = \varphi_i(T_0)$. At time $t \geq T_0 + 1$, noise $\theta_i(t)$ is constructed as

$$\theta_i(t) = \varphi_i(t) - \varphi_i(t-1), \forall t \geq T_0 + 1. \tag{12}$$

After deriving $\theta_i(t)$, DS i perturbs the updated state $y_i(t)$ using (6). Note that the noises in $\{\theta_i(t), \forall t \geq T_0\}$ are correlated. When a new state $\widetilde{y}_i(t)$ is published, the uncertainty in $\widetilde{y}_i(T_0)$ may change, leading to the variation of privacy protections in Step 2.

Similarly, we use $M_2^2 : \mathbb{R}^{m_i} \to \mathbb{R}$ to denote the privacy-preserving mechanism introduced by (12). Different from M_2^1, M_2^2 provides time-varying privacy protections in Step 2, which is shown in the following theorem.

***Theorem** 2.* Given $\alpha > 0$, at time $t \geq T_0$, the mechanism M_2^2 preserves $\frac{\alpha^2}{2\sum_{j=1}^{m_i}\sigma_{i,j}^2+2\left(\sum_{i=1}^{n} m_i/n\right)^2\rho^{t-T_0}\sigma_i^2}$-KLDP.

From the theorem, we observe that the PPL provided by M_2^2 increases with iterations. Recall that a larger PPL indicates weaker privacy guarantee. This also implies that the uncertainty in $\widetilde{y}_i(T_0)$ is reduced due to multiple releases of $\widetilde{y}_i(t)$. In particular, taking limitation on the PPL, we derive

$$\lim_{t\to\infty} \epsilon_2^2(t) = \frac{\alpha^2}{2\sum_{j=1}^{m_i}\sigma_{i,j}^2}. \tag{13}$$

Such kind of time-varying protection is satisfying since it takes a long time for eavesdroppers to make accurate inference and the final inferred result still contains strong privacy guarantee. It is easy to check that the PPL in (13) is still smaller than that of Step 1 (given in Lemma 1) if $m_i \geq 2$. Thus, in Step 2, DCs obtain stronger privacy protections in all iterations than those with Step 1.

Lemma 4 to be stated below gives the convergence property of Scheme 2. Here, we define some notations, which will be used in the lemma. First, we introduce vectors aggregating variables related to DSs. Let $\mathbf{y}(t) := [y_1(t)\cdots y_n(t)]^{\mathrm{T}}$, $\boldsymbol{\theta}(t) := [\theta_1(t)\cdots\theta_n(t)]^{\mathrm{T}}$, $\boldsymbol{\varphi}(t) := [\varphi_1(t)\cdots\varphi_n(t)]^{\mathrm{T}}$, and $\widetilde{\mathbf{x}} := \widetilde{x}\cdot\mathbf{1}_n$. Also, we use a matrix W with dimension $n \times n$ to aggregate all DSs' weights defined in (3), i.e., $W := [w_{il}]$. For weight matrix W, we denote its eigenvalues as $\lambda_1, \cdots, \lambda_n$. Under (3), there is only one eigenvalue equal to 1 while others are less than 1 in magnitude. Without loss of generality, we assume $\lambda_1 = 1$, and thus, $\lambda_i < 1, \forall i \neq 1$. In addition, the maximum variance of noises $\theta_i(T_0), \forall i$, is denoted by $\sigma_{\max}^2$, namely, $\sigma_{\max}^2 := \max_{i\in\mathcal{V}}\sigma_i^2$. We also use $\mathrm{tr}[\cdot]$ to denote the trace of a matrix.

***Lemma** 4.* If all DSs use (7) to update states, where the noises $\theta_i(t), \forall i$, are set by (12), then the states of DSs converge to $\widehat{x}$ in the mean-square sense, i.e.,

$$\lim_{t\to\infty} \mathbb{E}_{\{\boldsymbol{\theta}(t)\}}\|\mathbf{y}(t) - \widehat{\mathbf{x}}\|_2^2 = 0. \tag{14}$$

We can also deduce that Scheme 2 achieves convergence in expectation. Mean-square convergence is stronger than the former one though the expense is that the provided privacy protection becomes weaker.

3.3 Scheme 3: Zero-sum bounded noises perturbation

In this subsection, we will introduce yet another approach, called Scheme 3. This one achieves asymptotic convergence, i.e., $\lim_{t\to\infty} y_i(t) = \widehat{x}, \forall i$. We also adopt the idea of zero-sum noises perturbation, but the used noises are bounded. Denote the bound of initial noise $\boldsymbol{\varphi}(T_0)$ as a, that is, $\|\boldsymbol{\varphi}(T_0)\|_\infty \leq a$. Also, there exists a decaying rate $\rho \in (0,1)$ such that $\|\boldsymbol{\varphi}(t)\|_\infty \leq a\rho^{t-T_0}, \forall t \geq T_0$. Then, $\theta_i(t)$ is constructed as

$$\theta_i(t) = \begin{cases} \varphi_i(T_0), & t = T_0, \\ \varphi_i(t) - \varphi_i(t-1), & t > T_0. \end{cases} \tag{15}$$

For example, $\varphi_i(t), t \geq T_0$, can be set as $\varphi_i(t) \sim U[-a\rho^{t-T_0}, a\rho^{t-T_0}]$, where $U[\cdot]$ denotes the uniform distribution. In this paper, we only require that the noises in (15) are zero-sum and their bounds decay with iterations, but do not specify the distributions. Thus, the analysis about privacy and convergence will be conducted without using the noise distributions.

The scheme in (15) is also denoted by a privacy-preserving mechanism $M_2^3 : \mathbb{R}^{m_i} \to \mathbb{R}$. The following lemma shows its privacy protection.

***Lemma** 5.* Given $\alpha > 0$, the mechanism M_2^3 preserves $\frac{\alpha^2}{2\sum_{j=1}^{m_i}\sigma_{i,j}^2}$-KLDP when $t \to \infty$.

***Remark** 1.* The PPL $\epsilon_2^3(t)$ provided by M_2^3 also increases with iterations and finally converges to $\alpha^2/2\sum_{j=1}^{m_i}\sigma_{i,j}^2$. Since the distribution of the noises added in Scheme 3 is not specified, we do not give the closed-form PPLs in each iteration. Lemma 5 provides the upper bound of these PPLs, which is the same with that of Scheme 2.

Nevertheless, Scheme 2 provides stronger protection in each iteration than Scheme 3 since the latter adopts bounded noises for perturbation.

Theorem 3 to be stated below presents the convergence property of Scheme 3. Before giving the theorem, we first introduce a lemma from Seneta (2006), which will be used for the proof. In what follows, for a vector $\mathbf{x}$, we use $\max(\mathbf{x})$ and $\min(\mathbf{x})$ to denote its maximum and minimum elements, respectively. Then, let $V(\mathbf{x}) := \max(\mathbf{x}) - \min(\mathbf{x})$.

***Lemma** 6.* For a stochastic matrix $W \in \mathbb{R}^{n\times n}$ and a vector $\mathbf{x} \in \mathbb{R}^n$, it holds

$$V(W\mathbf{x}) \leq \left(\frac{1}{2}\max_{i,j}\sum_{l=1}^{n}\left|[W]_{il} - [W]_{jl}\right|\right) V(\mathbf{x}).$$

For simplicity, let $\chi := \frac{1}{2}\max_{i,j}\sum_{l=1}^{n}\left|[W]_{il} - [W]_{jl}\right|$. According to (3), we know $\chi \in (0, 1)$.

***Theorem** 3.* If all DSs use (7) to update their states, where the noises $\theta_i(t), \forall i$, are set by (15), then the states of DSs asymptotically converge to $\widehat{x}$, i.e.,

$$\lim_{t\to\infty} \mathbf{y}(t) = \widehat{\mathbf{x}}. \tag{16}$$

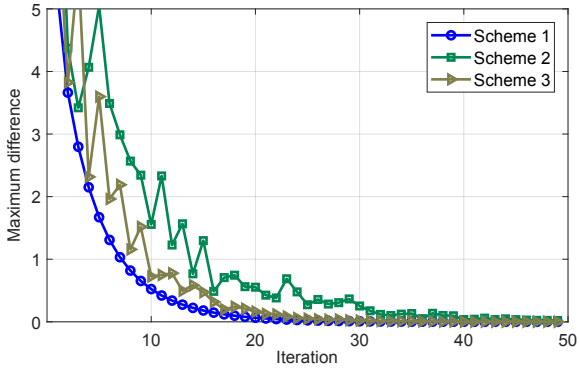
Theorem 3 states that Scheme 3 achieves asymptotic convergence in a deterministic sense, which is the strongest convergence guarantee among the three schemes.

3.4 Discussions

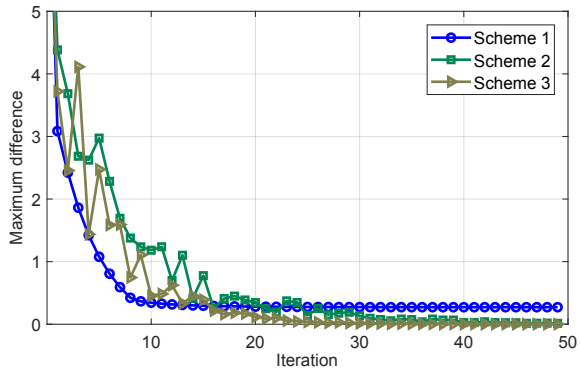
The idea of zero-sum noises perturbation is also adopted by Mo and Murray (2017) and He et al. (2019), where the data reporting process of DCs is not considered, leading to the failure for achieving heterogeneous privacy guarantee. Moreover, we analyze the privacy properties using KLDP, whose PPL is measured by the similarity of distributions of published information, not in the sense of estimation probabilities considered in the literature. KLDP gives an inherent limit on these estimation probabilities, and the closed-form of PPL can be derived once the noises for perturbation are chosen. In this paper, we analyze the dynamic characteristics of privacy loss and provide the theoretical PPL in each iteration, which is also a new contribution compared with existing works.

There exists a tradeoff between privacy preservation and convergence guarantee. That is, a private mechanism with stronger protection achieves weaker convergence guarantee. The schemes proposed in this paper achieve different privacy and convergence performances, providing DCs and DSs diverse choices for collaborative computing. We give more details regarding these aspects below.

Privacy preservation. First, the three schemes provide DCs with the same privacy guarantee in Step 1 since they use a common perturbation approach there. However, they offer different protections in Step 2. Specifically, Scheme 1 protects the strongest privacy, and the guarantee does not vary with iterations. In contrast, Schemes 2 and 3 achieve time-varying protections, and their final PPLs are the same. Since the noises for perturbation are unbounded, Scheme 2 provides stronger preservation than Scheme 3 in each iteration. It is emphasized that whichever of the three mechanisms is used, the PPLs in Step 2 are less than that in Step 1. This implies heterogeneous privacy guarantee is successfully achieved by all three schemes.



(a) Maximum difference between states



(b) Maximum deviation between states and $\hat{x}$

Fig. 1. Convergence guarantees of different schemes.

Convergence guarantee. By the three schemes, DSs' states converge to the average value of all reported data, i.e., $\widehat{x}$. Though the convergence is with respect to $\widehat{x}$, their convergence guarantees are distinct. Scheme 1 achieves convergence in the sense of expectation, which is the weakest among the three schemes. Actually, if the average of $\widetilde{y}_i(T_0)$ is set as the reference value, Scheme 1 achieves asymptotic convergence. Mean-square convergence guarantee is offered by Scheme 2 while under Scheme 3, DSs' states converge to $\widehat{x}$ for sure. Therefore, Schemes 1, 2 and 3 achieve convergence guarantees from weak to strong.

4. EVALUATION

System settings We use a connected network of $n = 20$ DSs as the underlying communication topology. Each DS is assumed to collect data from a group of $m_i = 100$ DCs. The private data of a DC is set to an integer, which is randomly sampled from $[1, 100]$. After these settings, we can compute the true average value of all DCs' data as $\overline{x} = 50.45$. Suppose that in Step 1 all DCs have the same PPL, and we set it as $\epsilon_1 = 0.5$. For the adjacent distance α, considering the distribution of the original data, we set it to 2. Then, we have $\sigma_{i,j}^2 = 4, \forall i, j$. Let all DCs use (5) to obfuscate their data, and then the average value computed by the three schemes is $\widehat{x} = 50.41$.

In Step 2, all three schemes adopt the same variance for initial noise $\theta_i(T_0)$ and set it to 9, i.e., $\sigma_i^2 = 9, \forall i$. The

decaying rate ρ used in Schemes 2 and 3 is chosen as 0.8. For the bounded noises leveraged in Scheme 3, we utilize uniform distribution shown in Section 3.3. In the simulations, each scheme was run for 5,000 times.

Simulation results We compare the convergence properties of the three schemes. Fig. 1(a) illustrates the maximum distances between arbitrary two DSs' states when different privacy-aware schemes are applied. We find that all the distances converge to 0, which implies that states consensus is achieved by all three schemes. However, concerning the final values, we observe distinct convergence guarantees, as shown in Fig. 1(b). Under Scheme 1, there exists a non-zero gap between DSs' final value and $\widehat{x}$, since this scheme only achieves convergence in expectation. In contrast, such a gap is not present when the other two schemes are used. Hence, in the sense of convergence guarantee, Schemes 2 and 3 are better than Scheme 1, which reconciles with our theoretical results.

5. CONCLUSION

In this paper, we have proposed three different privacy-aware schemes for a collaborative computing framework. On the basis of heterogeneous protections, the proposed schemes have been proved to preserve dynamic privacy as iterations proceed. Further, their PPLs in different iterations have been derived. Moreover, we have proved that all three schemes achieve convergence, but their guarantees are different, which are related to the strength of privacy protections. Finally, the obtained theoretical results have been validated by a numerical example. For future works, we intend to extend our privacy-aware schemes to statistical analysis of real-time streaming data.

REFERENCES

Asghar, M.R., Dán, G., Miorandi, D., and Chlamtac, I. (2017). Smart meter data privacy: A survey. *IEEE Communnication Surveys and Tutorials*, 19(4), 2820–2835.

Bullo, F. (2019). *Lectures on Network Systems*. Kindle Direct Publishing.

Cisco (2018). Cisco global cloud index: Forecast and methodology, 2016-2021 white paper.

Cuff, P. and Yu, L. (2016). Differential privacy as a mutual information constraint. In *Proceedings of ACM SIGSAC Conference on Computer and Communications Security*, 43–54.

Duan, X., He, J., Cheng, P., Mo, Y., and Chen, J. (2015). Privacy preserving maximum consensus. In *Proceedings of 54th IEEE Conference on Decision and Control*, 4517–4522.

Dwork, C. (2008). Differential privacy: A survey of results. In *Proceedings of International Conference on Theory and Applications of Models of Computation*, 1–19.

Fredrikson, M., Lantz, E., Jha, S., Lin, S., Page, D., and Ristenpart, T. (2014). Privacy in pharmacogenetics: An end-to-end case study of personalized warfarin dosing. In *23rd USENIX Security Symposium*, 17–32.

Gade, S. and Vaidya, N.H. (2018). Privacy-preserving distributed learning via obfuscated stochastic gradients. In *Proceedings of 57th IEEE Conference on Decision and Control*, 184–191.

He, J., Cai, L., Cheng, P., Pan, J., and Shi, L. (2019). Consensus-based data-privacy preserving data aggregation. *IEEE Transactions on Automatic Control*. Doi: 10.1109/TAC.2019.2910171.

Hsieh, K., Harlap, A., Vijaykumar, N., Konomis, D., Ganger, G.R., Gibbons, P.B., and Mutlu, O. (2017). Gaia: Geo-distributed machine learning approaching LAN speeds. In *USENIX Symposium on Networked Systems Design and Implementation*, 629–647.

Huang, Z., Mitra, S., and Dullerud, G. (2012). Differentially private iterative synchronous consensus. In *Proceedings of ACM Workshop on Privacy Electronic Society*, 81–90.

Mo, Y. and Murray, R.M. (2017). Privacy preserving average consensus. *IEEE Transactions on Automatic Control*, 62(2), 753–765.

Nozari, E., Tallapragada, P., and Cortés, J. (2017). Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design. *Automatica*, 81, 221–231.

Qin, Z., Yu, T., Yang, Y., Khalil, I., Xiao, X., and Ren, K. (2017). Generating synthetic decentralized social graphs with local differential privacy. In *Proceedings of ACM SIGSAC Conference on Computer and Communications Security*, 425–438.

Ruan, M., Gao, H., and Wang, Y. (2019). Secure and privacy-preserving consensus. *IEEE Transactions on Automatic Control*, 64(10), 221–231.

Seneta, E. (2006). *Non-negative Matrices and Markov Chains*. Springer.

Smith, V., Chiang, C.K., Sanjabi, M., and Talwalkar, A.S. (2017). Federated multi-task learning. In *Advances in Neural Information Processing Systems*, 4424–4434.

Wang, X., He, J., Cheng, P., and Chen, J. (2019a). Differentially private maximum consensus: Design, analysis and impossibility result. *IEEE Transactions on Network Science Engineering*, 6(4), 928–939.

Wang, X., He, J., Cheng, P., and Chen, J. (2019b). Privacy preserving collaborative computing: Heterogeneous privacy guarantee and efficient incentive mechanism. *IEEE Transactions on Signal Processing*, 67(1), 221–233.

Wang, X., Ishii, H., Du, L., Cheng, P., and Chen, J. (2019c). Differential privacy-preserving distributed machine learning. Proceedings of 58th IEEE Conference on Decision and Control.

Xiao, L., Boyd, S., and Lall, S. (2005). A scheme for robust distributed sensor fusion based on average consensus. In *Fourth International Symposium on Information Processing in Sensor Networks*, 63–70.