Adaptive Differentially Quantized Subspace Perturbation (ADQSP)
A Unified Framework for Privacy-Preserving Distributed Average Consensus

Li, Qiongxiu; Gundersen, Jaron Skovsted; Lopuhaa-Zwakenberg, Milan; Heusdens, Richard

DOI
10.1109/TIFS.2023.3343599

Publication date
2024

Document Version
Final published version

Published in
IEEE Transactions on Information Forensics and Security

Adaptive Differentially Quantized Subspace Perturbation (ADQSP): A Unified Framework for Privacy-Preserving Distributed Average Consensus

Qiongxiu Li, *Member, IEEE*, Jaron Skovsted Gundersen, Milan Lopuhaä-Zwakenberg, and Richard Heusdens, *Senior Member, IEEE*

***Abstract*— Privacy-preserving distributed average consensus has received significant attention recently due to its wide applicability. Based on the achieved performances, existing approaches can be broadly classified into perfect accuracy-prioritized approaches such as secure multiparty computation (SMPC), and worst-case privacy-prioritized approaches such as differential privacy (DP). Methods of the first class achieve perfect output accuracy but reveal some private information, while methods from the second class provide privacy against the strongest adversary at the cost of a loss of accuracy. In this paper, we propose a general approach named adaptive differentially quantized subspace perturbation (ADQSP) which combines quantization schemes with so-called subspace perturbation. Although not relying on cryptographic primitives, the proposed approach enjoys the benefits of both accuracy-prioritized and privacy-prioritized methods and is able to unify them. More specifically, we show that by varying a single quantization parameter the proposed method can vary between SMPC-type performances and DP-type performances. Our results show the potential of exploiting traditional distributed signal processing tools for providing cryptographic guarantees. In addition to a comprehensive theoretical analysis, numerical validations are conducted to substantiate our results.**

***Index Terms*— Secure multiparty computation, differential privacy, decentralized networks, subspace perturbation, data aggregation, consensus, quantization.**

I. Introduction

AS THE world is becoming increasingly interconnected and digitized, data are often collected and stored in personal devices such as tablets and phones [1]. To process such massive amounts of data over different devices poses many challenges including: (1) the requirement for distributed processing tools that are able to process data in a network of devices without any centralized coordination; (2) the need for lightweight solutions as these devices are often limited in computational resources, and (3) the demand for privacy-preserving algorithms, as these devices often contain sensitive personal data captured by sensors such as images and GPS data [1]. Combined, these challenges call for interdisciplinary research across different fields such as cryptography, information theory and distributed signal processing for developing efficient and privacy-preserving distributed computation methods.

The average consensus problem has been intensively investigated and widely applied in many applications, e.g., optimization [2], group coordination [3], and federated learning [4]. Recently, privacy-preserving distributed average consensus, which aims to guarantee all participants in a network to output an accurate average consensus without violating privacy concerns, has received a lot of attention [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24]. There are at least five aspects to be considered when designing privacy-preserving distributed average consensus algorithms: centralized vs. decentralized coordination, computational complexity, communication costs, and most importantly, the achieved privacy level and output accuracy. With respect to the first concern, in this paper we only consider fully distributed/decentralized solutions which do not require any centralized coordination such as a trusted third party. Secondly, the computational complexity depends heavily on the so-called security model, i.e., whether we demand computational or information-theoretical security. In this work, we will restrict ourselves to information-theoretical security based algorithms since they are generally computationally less complex compared to computational security based approaches as the former does not involve complex encryption operations.

With respect to communication cost, privacy, and accuracy, most existing work focuses on privacy and accuracy, while the aspect of communication cost is rarely addressed. Ideally, one would like perfect accuracy while guaranteeing privacy even against the strongest adversary, which is all participants except one collude. This, however, has been shown to be impossible [25]. The main reason is that having knowledge of the average result will reveal the private data held by the only non-colluding participant. As a result, existing

Manuscript received 17 July 2023; revised 2 November 2023; accepted 11 December 2023. Date of publication 15 December 2023; date of current version 26 December 2023. This work was supported in part by the European Union's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie under Grant 101008233 and in part by ERC Consolidator under Grant 864075 "Caesar". The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Diana Pamela Moya Osorio. *(Corresponding author: Qiongxiu Li.)*

Qiongxiu Li is with the Department of Computer Science, Tsinghua University, Beijing 100190, China (e-mail: qiongxiuli@mail.tsinghua.edu.cn).

Jaron Skovsted Gundersen is with the Department of Electronic Systems, Aalborg University, 9220 Aalborg, Denmark (e-mail: jaron@es.aau.dk).

Milan Lopuhaä-Zwakenberg is with the Department of Mathematics and Computer Science, University of Twente, 7522 NB Enschede, The Netherlands (e-mail: m.a.lopuhaa@utwente.nl).

Richard Heusdens is with the Netherlands Defence Academy (NLDA), 1781 AC Den Helder, The Netherlands, and also with the Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, 2628 CD Delft, The Netherlands (e-mail: r.heusdens@tudelft.nl).

Digital Object Identifier 10.1109/TIFS.2023.3343599

work falls into two categories. The first category contains algorithms that guarantee privacy against the worst-case adversary using differential privacy (DP) techniques [26], [27] by inserting noise into the calculations [10], [11], [12], [13]. This guarantees one individual's privacy even when all other participants are compromised, at the cost of output accuracy. The second category contains secure multiparty computation (SMPC) based approaches like secret sharing [14], [15], [16], [17] and correlated noise insertion [20], [21], [22], which offer perfect accuracy but only guarantee privacy under additional assumptions on the set of compromised participants.

A. Paper Contribution

In this paper, we present a communication efficient algorithm that links the performances of SMPC and DP approaches in a unified framework. Our key results are summarized as follows:

1) We analyze the problem of privacy-preserving distributed average consensus over networks and prove two impossibility results about the performances of privacy and accuracy given the network topology. In particular, we prove that the so-called ideal world defined in SMPC is impossible to achieve if the adversary disconnects the network.
2) We propose a novel approach, referred to as *adaptive differentially quantized subspace perturbation (ADQSP)*, by combining the potential of quantization schemes and the subspace perturbation technique. It enjoys superior performance compared to existing approaches in terms of accuracy, privacy and communication efficiency.
3) We show that our proposed approach can achieve SMPC and (relaxed) DP performances by appropriate parameter settings. To the best of our knowledge, the proposed approach is the first information-theoretical approach that unifies both SMPC and DP in this context.

Both theoretical investigations and numerical validations are presented to consolidate our claims. We published preliminary results in [28] where only the connection of quantized subspace perturbation and DP is shown. In this paper we show that the proposed ADQSP approach can achieve both SMPC and DP related performances. In addition, we give a complete information-theoretical analysis of privacy via mutual information.

B. Outline and Notation

The paper is organized as follows. In Section II, we introduce the problem setup and define the adversary model and privacy metrics. In Section III, we analyze the problem at hand and prove two impossibility results regarding the performances. In Section IV, we introduce the proposed approach. In Section V, we analyze the performance of existing SMPC and DP approaches, while in Section VI, we analyze the performance of the proposed approach and show that by tuning a single parameter the performance can vary between that of SMPC and (relaxed) DP. Numerical validations are demonstrated in Section VII and conclusions are drawn in Section VIII.

We use bold letters for vectors ($\boldsymbol{x}$) and matrices ($\boldsymbol{X}$), where capital letters are used for matrices. Sets are denoted by calligraphic letters ($\mathcal{X}$). $\boldsymbol{I}$ denotes the identity matrix. We refer to the i-th entry of a vector $\boldsymbol{x}$ as x_i.[1] With a slight abuse of notation, we denote a random variable by a capital letter X no matter if the outcome is a scalar x, a vector $\boldsymbol{x}$, or a matrix $\boldsymbol{X}$.

II. Preliminaries

In this section we review some necessary fundamentals for the remainder of the paper.

A. Privacy-Preserving Distributed Average Consensus

A network is modelled as a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \{1, \ldots, n\}$ is the set of vertices representing the nodes/agents/participants in the network, and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ is the set of $m := |\mathcal{E}|$ (undirected) edges, representing the communication links in the network. The set of neighbors of node i is denoted as $\mathcal{N}_i = \{j \mid (i, j) \in \mathcal{E}\}$ and its degree is $d_i = |\mathcal{N}_i|$. A graph is connected if for every pair of nodes there is a path between them. In this paper, for the feasibility of the average output, we assume the graph $\mathcal{G}$ is connected.

Assume each node $i \in \mathcal{V}$ in the network holds private data s_i. The goal of privacy-preserving distributed average consensus is to allow each node to obtain the average of all private data over the network, i.e.,

$$s_{\text{ave}} = \frac{1}{n} \sum_{i \in \mathcal{V}} s_i, \tag{1}$$

without revealing each node's private data and without any centralized coordination.

B. Adversary Model

In this paper we consider both the well-known eavesdropping adversary and the so-called passive (i.e., honest-but-curious) adversary. Throughout the paper, we assume these two adversaries can cooperate by sharing information to increase the chance of inferring private data. The eavesdropping adversary works by eavesdropping all communication channels (edges) between nodes in the network. The passive adversary is assumed to be able to corrupt a subset of the nodes, referred to as *corrupt nodes*. The nodes that are not corrupt, on the other hand, are referred to as *honest nodes*. The corrupt nodes are assumed to not deviate from the protocol, but collect all information they see throughout the protocol. The collected information includes for example the inputs of the corrupt nodes and the messages they receive during the computation from neighboring nodes. Denote the set of honest nodes as $\mathcal{V}_h$ and the corrupt nodes as $\mathcal{V}_c$. We let $\mathcal{E}_h = \{(i, j) \in \mathcal{E} \mid i, j \in \mathcal{V}_h\}$ be the set of edges between two honest nodes and $\mathcal{E}_c = \mathcal{E} \setminus \mathcal{E}_h$ be the set of edges containing at least one corrupt node. Furthermore, the set of honest neighbors of node i is denoted by $\mathcal{N}_{i,h} = \{j \mid (i, j) \in \mathcal{E}_h\}$.

C. Performance Evaluation and Corresponding Metrics

To evaluate the performance of a privacy-preserving algorithm, there are at least two key requirements.

[1]For simplicity we assume that the entries x_i are scalar variables but the results can easily be generalized to arbitrary dimensions.

1) Output Accuracy: The output accuracy measures how good the functionality of the algorithm is. A typical way to quantify the output accuracy is to adopt some distance measures to evaluate "how far" the output of the privacy-preserving algorithm is, denoted as $\tilde{\boldsymbol{y}} \in \mathbb{R}^n$, to the desired output $\boldsymbol{y} \in \mathbb{R}^n$. In this paper we use the mean squared error (MSE) to quantify the output accuracy as it is widely used for iterative processes. It is defined as:

$$e = \frac{1}{n} ||\tilde{\boldsymbol{y}} - \boldsymbol{y}||^2 . \tag{2}$$

2) Individual Privacy: Individual privacy measures how well the private data of an honest node is being protected against the considered adversaries. Since the approaches considered here are information-theoretical ones, privacy should also be quantified using an information-theoretical measure. Widely used information-theoretical metrics for assessing privacy loss include for example ϵ-differential privacy and mutual information [29]. In this paper we adopt mutual information as our primary privacy metric for two main reasons. Firstly, its efficacy has been demonstrated in the realm of privacy-preserving distributed processing and in various applications [25], [30]. Secondly, it has been shown in [31] and [32] that mutual information is a relaxed version of ϵ-differential privacy (thus in Section V we refer that our proposed approach can achieve performances of relaxed DP approaches). And it is easier to implement mutual information in practice [33]. Considering two (continuous) random variables X and Y, the mutual information is defined by

$$\mathrm{I}(X; Y) = h(X) - h(X|Y), \tag{3}$$

where $h(X)$ denotes the differential entropy of X and $h(X|Y)$ is the conditional differential entropy, assuming they exist.[2] We have that $\mathrm{I}(X; Y) = 0$ when X and Y are independent, meaning that Y does not carry any information about X and $\mathrm{I}(X; Y)$ is maximal when there is a one-to-one relation between Y and X.

III. Problem Analysis and Impossibility Results

In this section we prove two impossibility results, showing that in distributed average consensus 1) the twin goals of perfect accuracy and worse-case privacy guarantee cannot be achieved simultaneously; 2) if the subgraph of honest nodes is disconnected, then no protocol can achieve the performances of the case where a trusted third party (TTP) is assumed to be available. These two results are related to the performances of two well-established privacy-preserving techniques: DP and SMPC, respectively. Without loss of generality, throughout the paper, we assume the following (recall the private data s_i is a realization of random variable S_i).

Assumption 1: All private data are statistically independent, i.e., $\forall i, j \in \mathcal{V}, i \neq j : \mathrm{I}(S_i; S_j) = 0$.

Assumption 2: The size of the network $n = |\mathcal{V}|$ *is known to all nodes. Hence, knowing the average of the data implies knowing the total sum and vice versa.*

We have the following results.

[2]In the case of discrete random variables we replace both differential entropies by the Shannon entropy so that $I(X; Y) = H(X) - H(Y|X)$.

A. Impossibility Result I: Perfect Accuracy and Worst-Case Privacy Cannot be Achieved Simultaneously

Lemma 1: By assuming perfect accuracy and worst-case privacy, i.e., $\mathcal{V}_c = \mathcal{V} \setminus \{i\}$, *the individual privacy leakage becomes*

$$\mathrm{I}(S_i; \sum_{j\in\mathcal{V}} S_j, \{S_j\}_{j\in\mathcal{V}_c}) = \mathrm{I}(S_i; S_i), \tag{4}$$

which is maximal.

The proof follows trivially from the fact that $\sum_{j\in\mathcal{V}} S_j - \sum_{j\in\mathcal{V}_c} S_j = S_i$ [25]. Similar results have also been proved via different metrics such as differential privacy [10]. Thus, if there are $n-1$ corrupt nodes, it is impossible to achieve any privacy for the only remaining honest node without compromising accuracy. Hence, there is an inherent trade-off between privacy and accuracy for differential privacy related approaches.

B. Impossibility Result II: An SMPC-Like Ideal World Cannot be Achieved Unless All Honest Nodes Are Connected

In SMPC, the *ideal world* describes the setting in which a TTP is assumed to be available. The TTP will (securely) collect all private data from each node and then compute the output of the function and send back the output to the nodes. However, in practice a TTP might not exist. The goal of SMPC is to design a protocol to replace a TTP. In the context of average consensus, as the corrupt nodes have available both their own private data and the average result, the information observed by the adversary in an ideal world setting is given by:

$$\mathcal{O}_{\text{ideal},\mathcal{V}_c} = \{S_i\}_{i\in\mathcal{V}_c} \cup \{\sum_{i\in\mathcal{V}} S_i\}. \tag{5}$$

Hence, for an arbitrary honest node $i \in \mathcal{V}_h$ we have

$$\mathrm{I}(S_i; \mathcal{O}_{\text{ideal},\mathcal{V}_c}) = \mathrm{I}(S_i; \sum_{i\in\mathcal{V}_h} S_i). \tag{6}$$

Hence, a perfect SMPC protocol for privacy-preserving distributed average consensus outputs the correct average value and guarantees that the adversary obtains no more information about the honest nodes' private data than (6). The following result shows that such a protocol cannot exist when the honest nodes do not form a connected subgraph.

Proposition 1: Let $\mathcal{G}_h = (\mathcal{V}_h, \mathcal{E}_h)$ *be the subgraph of* $\mathcal{G}$ *obtained by removing all corrupt nodes. Let* $\mathcal{G}_{h,1}, \ldots, \mathcal{G}_{h,k_h}$ *be the components (connected subgraphs that are not part of any larger connected subgraph) of* $\mathcal{G}_h$ *and let* $\mathcal{V}_{h,k}$ *denote the vertex set of* $\mathcal{G}_{h,k}$.

Then for any protocol outputting $f(s_1, s_2, \ldots, s_n) = \sum_{i=1}^n s_i$ *to all nodes, after the protocol the adversary will always have learned* $\{\sum_{i\in\mathcal{V}_{h,k}} S_i\}_{k=1,2,\ldots,k_h}$.

Proof: See Appendix C. □

In other words, any algorithm with perfect accuracy will always leak the partial sums of the components of $\mathcal{G}_h$ to the adversary. Note that $\mathcal{G}_h$ is very likely to be disconnected in incomplete networks, especially in the presence of a lot of corrupt nodes. Hence, a perfect SMPC protocol for privacy-preserving distributed average consensus does not exist if the adversary disconnects the honest nodes [34].

C. Redefined Ideal World for Incomplete Networks

Using Proposition 1, we can derive a tighter bound on the information view of the adversary by taking the network topology into account, which we refer to as the redefined ideal world. The information observed by the adversary in this redefined ideal world setting, referred to as $\mathcal{O}_{\text{reideal}}$, is

$$\mathcal{O}_{\text{reideal},\mathcal{V}_c} = \{S_j\}_{j\in\mathcal{V}_c} \cup \{\sum_{i\in\mathcal{V}_{h,k}} S_i\}_{k=1,2,\ldots,k_h}. \tag{7}$$

Hence, since $\mathcal{V}_{h,k} \subseteq \mathcal{V}_h$ we have $\mathrm{I}(S_i; \mathcal{O}_{\text{reideal},\mathcal{V}_c}) \geq \mathrm{I}(S_i; \mathcal{O}_{\text{ideal},\mathcal{V}_c})$ and equality holds if and only if the subgraph $\mathcal{G}_h$ is connected, i.e., if $k_h = 1$.

For the simplicity of notation, assume that the honest node i belongs to the first honest component, i.e., $i \in \mathcal{V}_{h,1}$. We conclude that a perfect SMPC protocol should reveal no more information about s_i than

$$\mathrm{I}(S_i; \mathcal{O}_{\text{reideal},\mathcal{V}_c}) = \mathrm{I}(S_i; \sum_{j\in\mathcal{V}_{h,1}} S_j). \tag{8}$$

IV. Proposed ADQSP Protocol

The proposed ADQSP is constructed from two building blocks in distributed optimization, namely *adaptive differential quantization* [28], [35] and *subspace perturbation* [18], [19]. In what follows, we first briefly introduce the fundamentals of distributed optimization and these two building blocks, and afterwards we explain the details of the proposed approach.

A. Distributed Optimization

To solve (1) in a distributed manner, we first formulate it as a constrained optimization problem:

$$\begin{aligned} &\min_{\{x_1,\ldots,x_n\}} \sum_{i\in\mathcal{V}} \frac{1}{2}\|x_i - s_i\|^2 \\ &\text{s.t.} \quad \forall (i,j)\in\mathcal{E}: \; x_i = x_j, \end{aligned} \tag{9}$$

where x_i is a local optimization variable at node i with optimal value $x_i^* = s_{\text{ave}}$. A typical way to solve the above problem is to apply a solver like ADMM [36] or PDMM [37], [38]. As shown in [38] these distributed optimization algorithms can be described in a general framework using monotone operator theory [39] and operator splitting techniques.

For average consensus, the local updating functions are given by

$$x_i^{(t+1)} = \frac{s_i - \sum_{j\in\mathcal{N}_i} B_{i|j} z_{i|j}^{(t)}}{1 + cd_i} \tag{10}$$

$$z_{j|i}^{(t+1)} = \theta z_{j|i}^{(t)} + (1-\theta)\left(z_{i|j}^{(t)} + 2cB_{i|j}x_i^{(t+1)}\right). \tag{11}$$

Here $\boldsymbol{z}\in\mathbb{R}^{2m}$ is an auxiliary variable having entries indicated by $z_{i|j}$ and $z_{j|i}$, held by node i and j, respectively, related to edge $(i,j)\in\mathcal{E}$. The matrix $\boldsymbol{B}\in\mathbb{R}^{m\times n}$ is the graph incidence matrix and $B_{i|j}$ and $B_{j|i}$ are edge-related (scalar) weights, which are related to entries of $\boldsymbol{B}$ as $B_{k,i} = B_{i|j}$ and $B_{k,j} = B_{j|i}$ for $e_k = (i,j)$, i.e., the k-th edge in the graph. We will use the convention that $B_{i|j} = 1$ and $B_{j|i} = -1$ if $i < j$. In addition, $c > 0$ and $\theta \in [0,1)$ are constants, with c controlling the convergence rate and θ controlling the averaging of the (non-expansive) operators (recall that $d_i = |\mathcal{N}_i|$ is the degree of node i). The case $\theta = 0$ corresponds to PDMM and $\theta = 0.5$ corresponds to ADMM.

The protocol is summarized in Algorithm 1 where $t_{\max}$ denotes the maximum number of iterations. Note that there is also an alternative broadcast algorithm that requires only broadcasting of $x_i^{(t+1)}$'s to all neighbors, instead of exchanging the $z_{j|i}^{(t+1)}$'s one by one; the reception of $x_i^{(t+1)}$ is all that is needed for node $j\in\mathcal{N}_i$ to compute $z_{j|i}^{(t+1)}$ (see Appendix B for details).

Algorithm 1 Distributed Optimization for Average Consensus

At each $i\in\mathcal{V}$:
1) Initialize $z_{i|j}^{(0)} = 0$;
2) For $t = 0, 1, \ldots, t_{\max}-1$ do
   a) Compute $x_i^{(t+1)}$ and $\{z_{j|i}^{(t+1)}\}_{j\in\mathcal{N}_i}$ using (10) and (11), respectively;
   b) Send $z_{j|i}^{(t+1)}$ to neighbor $j\in\mathcal{N}_i$;
3) Output $x_i^{(t_{\max})}$

B. Subspace Perturbation

By inspection of (10), we can see that there can be two noise-insertion options to protect the private data s_i: adding noise to the optimization variable $\boldsymbol{x}\in\mathbb{R}^n$ directly or adding noise to the auxiliary variable $\boldsymbol{z}\in\mathbb{R}^{2m}$. The subspace perturbation approach adds noise to the auxiliary variable $\boldsymbol{z}$, as it often has more degrees of freedom [18], [19]. We have shown in previous work [19], [35] that only a part of $\boldsymbol{z}$ is predictable (like $\boldsymbol{x}$ converges to a value known by the adversary), while the other part is not. To explain this in more detail, we first write the local functions (10) and (11) in a compact form as follows:

$$\boldsymbol{x}^{(t+1)} = (\boldsymbol{I} + c\boldsymbol{C}^\top\boldsymbol{C})^{-1}(\boldsymbol{s} - \boldsymbol{C}^\top\boldsymbol{z}^{(t)}) \tag{12}$$

$$\boldsymbol{z}^{(t+1)} = \theta\boldsymbol{z}^{(t)} + (1-\theta)\left(\boldsymbol{P}\boldsymbol{z}^{(t)} + 2c\boldsymbol{P}\boldsymbol{C}\boldsymbol{x}^{(t+1)}\right), \tag{13}$$

where $\boldsymbol{C} = [\boldsymbol{B}_+^\top, \boldsymbol{B}_-^\top]^\top \in \mathbb{R}^{2m\times n}$ and $\boldsymbol{B}_+$ and $\boldsymbol{B}_-$ contains the positive and negative entries of $\boldsymbol{B}$, respectively. Furthermore, $\boldsymbol{P}\in\mathbb{R}^{2m\times 2m}$ is a permutation matrix switching the upper m rows and lower m rows of the matrix it operates on, i.e., $\boldsymbol{P}\boldsymbol{C} = [\boldsymbol{B}_-^\top, \boldsymbol{B}_+^\top]^\top$.

Let $\Psi = \mathrm{ran}(\boldsymbol{C}) + \mathrm{ran}(\boldsymbol{P}\boldsymbol{C})$, whose orthogonal complement is equal to $\Psi^\perp = \ker(\boldsymbol{C}^\top)\cap\ker((\boldsymbol{P}\boldsymbol{C})^\top)$. Moreover, let $\boldsymbol{\Pi}_\Psi$ be the orthogonal projection onto Ψ and let $\boldsymbol{z}_\Psi^{(t)} = \boldsymbol{\Pi}_\Psi\boldsymbol{z}^{(t)}$ and $\boldsymbol{z}_{\Psi^\perp}^{(t)} = (\boldsymbol{I} - \boldsymbol{\Pi}_\Psi)\boldsymbol{z}^{(t)}$. We then have the following decomposition

$$\boldsymbol{z}^{(t)} = \boldsymbol{z}_\Psi^{(t)} + \boldsymbol{z}_{\Psi^\perp}^{(t)}. \tag{14}$$

It has been proven in [35] that

$$\boldsymbol{z}_{\Psi^\perp}^{(t)} = \frac{1}{2}\left(\boldsymbol{z}_{\Psi^\perp}^{(0)} + \boldsymbol{P}\boldsymbol{z}_{\Psi^\perp}^{(0)}\right) + \frac{1}{2}(2\theta-1)^t\left(\boldsymbol{z}_{\Psi^\perp}^{(0)} - \boldsymbol{P}\boldsymbol{z}_{\Psi^\perp}^{(0)}\right).$$

Thus, for a given graph and θ, $\boldsymbol{z}_{\Psi^\perp}^{(t)}$ only depends on the initialization of the auxiliary variable $\boldsymbol{z}^{(0)}$. The main idea of subspace perturbation is to initialize $\boldsymbol{z}^{(0)}$ with a certain distribution having a sufficiently large variance, such that it can help to protect the private data from being revealed to

others (see Proposition 3 for details of the privacy proof). Moreover, by inspecting (12), we conclude that the $\boldsymbol{x}$-update is not affected by $\boldsymbol{z}_{\Psi^\perp}^{(t)}$ as $(\boldsymbol{z}_{\Psi^\perp}^{(t)})^\top \boldsymbol{C} = \boldsymbol{0}$. Hence, the output accuracy is not affected.

C. Adaptive Differential Quantization

Adaptive differential quantization schemes in distributed optimization were first introduced in [40] and [41]. They exploit the fact that when the algorithm converges, the difference between successive updates will converge to zero.

Let $Q^{(t)}\colon \mathbb{R} \to \{\Delta^{(t)}(a+1/2)\}_{a\in\mathcal{A}}$ denote an l-bit uniform (mid-rise) quantization function where $a \in \mathcal{A} = \{-2^{l-1}, -2^{l-1}+1, \ldots, 2^{l-1}-1\}$. Here $\Delta^{(t)}$ is the quantization cell-width which we define as

$$\Delta^{(t)} = \max\{\gamma^t \Delta^{(0)}, \Delta_{\min}\}, \tag{15}$$

where $\gamma \in (0,1)$ is a constant for controlling the decreasing rate, $\Delta^{(0)}$ denotes the initial cell-width and $\Delta_{\min}$ denotes the minimum cell-width. Given cell-width $\Delta^{(t)}$ at iteration t, $Q^{(t)}$ maps each input into its nearest representation value (midpoint of the quantization cells) in $\{\Delta^{(t)}(a+1/2)\}_{a\in\mathcal{A}}$.

Adaptive differential quantization does not operate on the auxiliary variable $\boldsymbol{z}$ directly but on the difference of successive variables. That is, let $\hat{\boldsymbol{z}}$ denote the quantized version of $\boldsymbol{z}$ and define $\Delta z_{j|i}^{(t+1)}$ as

$$\Delta z_{j|i}^{(t+1)} = \begin{cases} z_{j|i}^{(1)} - z_{j|i}^{(0)} & \text{if } t = 0 \\ z_{j|i}^{(t+1)} - \hat{z}_{j|i}^{(t)} & \text{if } t \geq 1. \end{cases} \tag{16}$$

and

$$\Delta \hat{z}_{j|i}^{(t+1)} = Q^{(t+1)}\left(\Delta z_{j|i}^{(t+1)}\right). \tag{17}$$

Upon receiving the quantized $\Delta\hat{z}_{j|i}$, each node then calculates $\hat{z}_{j|i}$ as

$$\hat{z}_{j|i}^{(t+1)} = \begin{cases} z_{j|i}^{(0)} + \Delta \hat{z}_{j|i}^{(1)} & \text{if } t = 0 \\ \hat{z}_{j|i}^{(t)} + \Delta \hat{z}_{j|i}^{(t+1)} & \text{if } t \geq 1. \end{cases} \tag{18}$$

Thus, the quantized $\hat{\boldsymbol{z}}$ can then be constructed as

$$\hat{\boldsymbol{z}}^{(t)} = \boldsymbol{z}^{(0)} + \sum_{\tau=1}^{(t)} \Delta \hat{\boldsymbol{z}}^{(\tau)}. \tag{19}$$

Às such, the quantized auxiliary variable $\hat{\boldsymbol{z}}^{(t+1)}$ cannot be reconstructed by the adversary until $\boldsymbol{z}^{(0)}$ is known.

The process of quantization will inevitably introduce distortion in the computations. Let $n_{j|i}^{(t+1)}$ denote the introduced error when quantizing $\Delta z_{j|i}^{(t+1)}$. We then have, by combining (16) and (18), that

$$\begin{aligned} n_{j|i}^{(t+1)} &= \Delta \hat{z}_{j|i}^{(t+1)} - \Delta z_{j|i}^{(t+1)} \\ &= \hat{z}_{j|i}^{(t+1)} - z_{j|i}^{(t+1)}. \end{aligned} \tag{20}$$

When implementing quantization, i.e., $\Delta z \to \Delta\hat{z}$, we apply a popular technique in quantization called dithering [42] when implementing the quantization function $Q^{(t)}$, this ensure that the quantization error is uniformly distributed over $[-\frac{\Delta^{(t)}}{2}, \frac{\Delta^{(t)}}{2}]$, and is independent of $\Delta z_{j|i}^{(t+1)}$, thus of $z_{j|i}^{(t+1)}$. In the coming Section VI-C we will show how this property benefits the privacy analysis.

D. Details of the Proposed Approach

Putting things together, the proposed approach first applies subspace perturbation and then adopts adaptive differential quantization to quantize the difference variable before updating. More specifically, at $t = 0$, subspace perturbation is applied by initializing $z_{i|j}^{(0)}$ at every node i with noise drawn from a distribution having large variance and sending it to neighbors $j \in \mathcal{N}_i$ via a securely encrypted channel. Each node i then updates its local variable $x_i^{(1)}$ and auxiliary variables $z_{j|i}^{(1)}$ according to (10) and (11), respectively, after which $\Delta z_{j|i}^{(1)}$ and $\Delta\hat{z}_{j|i}^{(1)}$ are computed using (16) and (17), respectively. After exchanging these quantities between neighboring nodes, $\Delta\hat{z}$ is computed as (18).

For $t \geq 1$, after achieving the quantized $\hat{z}_{i|j}^{(t)}$, each node i then repeats the following updating steps:

$$x_i^{(t+1)} = \frac{s_i - \sum_{j\in\mathcal{N}_i} B_{i|j}\hat{z}_{i|j}^{(t)}}{1 + cd_i} \tag{21}$$

$$\forall j \in \mathcal{N}_i : z_{j|i}^{(t+1)} = \theta \hat{z}_{j|i}^{(t)} + (1-\theta)\left(\hat{z}_{i|j}^{(t)} + 2cB_{i|j}x_i^{(t+1)}\right). \tag{22}$$

Note that except transmitting the initialized $\boldsymbol{z}^{(0)}$ all the communication channels do not require secure channel encryption when transmitting the quantized $\Delta\hat{\boldsymbol{z}}$, since from (19) we can see that the quantized $\hat{\boldsymbol{z}}^{(t)}$ cannot be reconstructed unless the initialized $\boldsymbol{z}^{(0)}$ is revealed (see Theorem 2 for detailed privacy proofs).

Algorithm 2 summarizes the details of the proposed approach. In the coming sections we will analyze the performance of the proposed approach and show its relation to both SMPC and DP.

Algorithm 2 Proposed ADQSP: Privacy-Preserving Distributed Average Consensus via Adaptive Differentially Quantized Subspace Perturbation

Initialization: Each node i randomly initializes $z_{i|j}^{(0)}$'s from independent Gaussian distributions[3] $\mathcal{N}(0;\sigma_z^2)$ for all $j \in \mathcal{N}_i$.
Input : Initialized auxiliary variables $\boldsymbol{z}^{(0)}$, quantization parameters $\Delta^{(0)}$, γ, $\Delta_{\min}$, l, and $t_{\max}$.
Output : Optimization solution: $x_i^{(t_{\max})}$
for $t = 0, 1, \ldots, t_{\max}-1$ **do**
  if $t = 0$ **then**
    Receive $z_{j|i}^{(0)}$ from $j \in \mathcal{N}_i$ via secure channels [43].
    $x_i^{(1)} \leftarrow$ (10), $\{z_{j|i}^{(1)}\}_{j\in\mathcal{N}_i} \leftarrow$ (11).
  end
  else
    Send $\Delta\hat{z}_{j|i}^{(t)}$ to $j \in \mathcal{N}_i$ via non-secure channels.
    $\{\hat{z}_{i|j}^{(t)}\}_{j\in\mathcal{N}_i} \leftarrow$ (18), $x_i^{(t)} \leftarrow$ (21),
    $\{z_{j|i}^{(t+1)}\}_{j\in\mathcal{N}_i} \leftarrow$ (22).
  end
  $\{\Delta\hat{z}_{j|i}^{(t+1)}\}_{j\in\mathcal{N}_i} \leftarrow$ (17), $\{\Delta z_{j|i}^{(t+1)}\}_{j\in\mathcal{N}_i} \leftarrow$ (16)
end

V. Information-Theoretical Analysis of Existing SMPC and DP Approaches

Before showing that the proposed ADQSP approach can obtain both SMPC and (relaxed) DP performances, we first introduce and analyze two example approaches of SMPC and DP. In particular, we will give an information theoretical analysis of individual privacy.

A. Performance Analysis of SMPC-Based Distributed Average Consensus

1) Application of Additive Secret Sharing in Distributed Average Consensus: Additive secret sharing is a popular SMPC technique. As an example, we now briefly explain how to apply additive secret sharing to distributed average consensus to achieve privacy-preservation [14], [16]. The basic idea is to encrypt the private data before performing averaging using a traditional average consensus algorithm such as Algorithm 1 or its broadcast alternative. Let $\mathbb{Z}_p$ be the cyclic group of p elements, represented by the integers $\{0, \ldots, p-1\}$. In order to apply additive secret sharing, we first need to transform all private data s_i to integers in $\mathbb{Z}_p$, where negative numbers are represented by their modular additive inverse and floating point numbers are scaled up into integers. In addition, p should be sufficiently large such that $p \geq \sum_{i\in\mathcal{V}} s_i$. Hence, discrete random variables are considered here. To apply additive secret sharing [44], each node i first chooses d_i elements $\{r_i^j \in \mathbb{Z}_p\}_{j\in\mathcal{N}_i}$ uniformly at random. It then sends r_i^j to node $j \in \mathcal{N}_i$ (which requires secure channel encryption) and computes its own share as

$$r_i^i = s_i - \sum_{j\in\mathcal{N}_i} r_i^j \mod p, \tag{23}$$

where r_i^i is a noisy version of the private data s_i. Two key properties of additive secret sharing, which we will prove using mutual information in Proposition 2, are: 1) the secret can only be reconstructed when all shares are known; 2) no information about the hidden secret can be inferred as long as one share is missing. We have the following result.

Proposition 2: (Properties of additive secret sharing) Let R_i^j be uniformly distributed in $\mathbb{Z}_p$ and let r_i^i be as in (23). Furthermore, let k be an element in $\mathcal{N}_i' = \mathcal{N}_i \cup \{i\}$. Then

$$\mathrm{I}(S_i; \{R_i^j\}_{j\in\mathcal{N}_i'}) = \mathrm{I}(S_i; S_i). \tag{24}$$

$$\mathrm{I}(S_i; \{R_i^j\}_{j\in\mathcal{N}_i'\setminus\{k\}}) = 0 \tag{25}$$

Proof: See Appendix D. □

In order to guarantee that adding noise to the original private data has no effect on the average result, each node i adds all received shares r_j^i from neighboring nodes to the share r_i^i. That is, node i constructs data s_i' as

$$\begin{aligned} s_i' &= r_i^i + \sum_{j\in\mathcal{N}_i} r_j^i \mod p \\ &= s_i + \sum_{j\in\mathcal{N}_i} (r_j^i - r_i^j) \mod p \end{aligned} \tag{26}$$

[3]Note that except for being independent, each node can choose its own noise distributions and variances, as long as they are sufficiently large for privacy guarantee.

and uses s_i' as input to Algorithm 1 (broadcast type). After obtaining the average of s_i', each node then constructs the final average output, denoted by s_{smpc}, as $s_{\mathrm{smpc}} = (n \times s_{\mathrm{ave}}' \mod p)/n$.

2) Output Accuracy: Since $\sum_{i\in\mathcal{V}}\sum_{j\in\mathcal{N}_i}(r_j^i - r_i^j) \mod p = 0$, the sum of s_i' is the same as the sum of s_i, i.e.,

$$\begin{aligned} \sum_{i\in\mathcal{V}} s_i' \mod p &= \sum_{i\in\mathcal{V}} \Big(s_i + \sum_{j\in\mathcal{N}_i}(r_j^i - r_i^j)\Big) \mod p \\ &= \sum_{i\in\mathcal{V}} s_i \end{aligned}$$

Thus, the MSE is then given by

$$\begin{aligned} e_{\mathrm{smpc}} &= (s_{\mathrm{smpc}} - s_{\mathrm{ave}})^2 \\ &= \Big(\frac{\sum_{i\in\mathcal{V}} s_i' \mod p}{n} - \frac{\sum_{i\in\mathcal{V}} s_i}{n}\Big)^2 = 0. \end{aligned}$$

Hence, output accuracy is not affected by applying additive secret sharing.

3) Individual Privacy: To analyze privacy, we need to first specify the view of the adversaries. In this analysis, we consider a scenario where each honest node has at least one corrupt neighbor. In that case, the view of the adversaries is given by

$$\mathcal{O}_{\mathrm{SMPC},\mathcal{V}_c} = \{S_j\}_{j\in\mathcal{V}_c} \cup \{R_j^k, R_k^j\}_{(j,k)\in\mathcal{E}_c} \cup \{X^{(t)}\}_{t\geq 1}.$$

With (10) and (11) we have that

$$\begin{aligned} & x_i^{(t+3)} - 2\theta x_i^{(t+2)} + (2\theta-1)x_i^{(t+1)} \\ &= \frac{-\sum_{j\in\mathcal{N}_i} B_{i|j}(z_{i|j}^{(t+3)} - 2\theta z_{i|j}^{(t+2)} + (2\theta-1)z_{i|j}^{(t+1)})}{1+cd_i} \\ &= \frac{-\sum_{j\in\mathcal{N}_i} 2c(1-\theta)((1-\theta)x_i^{(t+1)} + \theta x_j^{(t+1)} - x_j^{(t+2)})}{1+cd_i}. \end{aligned} \tag{27}$$

Hence, the adversary can compute $\boldsymbol{x}^{(t)}$ for $t \geq 3$ using the first two iterations ($t = 1, 2$). We have the following result.

Theorem 1: (Information loss of SMPC protocol) Assume that each honest node has at least one corrupt neighbor. Then computing averaging using inputs s_i' given by (26), the adversaries can infer the following information about an arbitrary honest node $i \in \mathcal{V}_h$:

$$\mathrm{I}(S_i; \mathcal{O}_{\mathrm{SMPC},\mathcal{V}_c}) = \mathrm{I}(S_i; \sum_{j\in\mathcal{V}_{h,1}} S_j).$$

Proof: See Appendix E and F. □

Hence, we conclude that the above SMPC approach achieves perfect output accuracy and the individual privacy reaches the bound (8) in the redefined ideal world, i.e.,

$$\left(e_{\mathrm{SMPC}} = 0, \mathrm{I}(S_i; \mathcal{O}_{\mathrm{SMPC},\mathcal{V}_c}) = \mathrm{I}(S_i; \sum_{j\in\mathcal{V}_{h,1}} S_j)\right). \tag{28}$$

B. Performance Analysis of DP-Based Distributed Average Consensus

In this section, we describe how DP-like methods [10], [11], [12] can be applied in average consensus. Specifically, this approach falls under *local differential privacy* (LDP) [45], in which there is no centralized server available and

each node considers all other nodes to be corrupt. The most straightforward way to incorporate LDP in distributed average consensus is via *local perturbation*: every node i draws a random noise r_i from some predetermined distribution, and adds it to its private data to obtain perturbed data, denoted as

$$\forall i \in \mathcal{V}: \ \tilde{s}_i = s_i + r_i \tag{29}$$

An average consensus protocol is then run on the perturbed data $\tilde{s}_i$ instead of the private data s_i.

1) Output Accuracy: Since distributed average consensus protocol is performed on $\tilde{s}_i$, its output is then given by $\frac{1}{n}\sum_i \tilde{s}_i$, so the MSE (2) is given by

$$e_{\text{DP}} = \frac{1}{n}\sum_{i=1}^{n}(\tilde{s}_i - s_i)^2 = \frac{1}{n}\sum_{i=1}^{n} r_i^2. \tag{30}$$

2) Individual Privacy: As explained before, mutual information is a relaxed version of ϵ-differential privacy [31], [32]. For consistency with the rest of this paper, here we also measure privacy leakages of DP approaches via mutual information. Therefore, we refer that our approach achieves performances of relaxed DP approaches. DP assumes that all nodes other than the considered node i are corrupt. In particular, the DP adversary knows $\tilde{s}_j$ for $j \neq i$ and, from the output of the average consensus protocol, also $\frac{1}{n}\sum_j \tilde{s}_j$. It follows that the DP adversary can always deduce $\tilde{s}_i$, and so individual privacy is given by

$$\text{I}(S_i; \mathcal{O}_{\text{DP},\mathcal{V}\setminus\{i\}}) = \text{I}(S_i; S_i + R_i). \tag{31}$$

Existing mechanisms give bounds to this, under assumptions of the distribution of the S_i. For instance, if it is known that $s_i \in [\alpha, \alpha + M]$ for $\alpha, M \in \mathbb{R}$, then taking r_i to follow the Laplace distribution with parameter M/ε ensures that (31) is bounded by ε [26]. Note that all noises R_i are independent of each other and their variances, denoted $\sigma_{r_i}^2$, is given by $\sigma_{r_i}^2 = 2M^2/\varepsilon^2$. Given (30), the variance of E_{DP} is thus

$$\frac{1}{n^2}\sum_{i=1}^{n}\sigma_{r_i}^2 = \frac{2M^2}{n\varepsilon^2}. \tag{32}$$

This shows that the more privacy we demand, i.e., the lower ε is, the less accurate the output average will be. Hence, there is a *privacy-accuracy trade-off* in DP approaches.

Overall, we conclude the output accuracy and individual privacy of a DP based approach is given by

$$\left(e_{\text{DP}} = \frac{1}{n}\sum_{i=1}^{n} r_i^2; \quad \text{I}(S_i; \mathcal{O}_{\text{DP},\mathcal{V}\setminus\{i\}}) = \text{I}(S_i; S_i + R_i)\right) \tag{33}$$

VI. Connection of Proposed Approach and Existing SMPC and DP Approaches

We first analyze the output accuracy and individual privacy of the proposed approach and then explain how it connects to existing SMPC and DP approaches.

A. Output Accuracy

As proved in [35], [40], and [41], the output accuracy is dependent on the parameter of $\Delta_{\min}$, i.e., minimum quantization cell-width. Let $r_{i,\min}$ denote the residual error in the output of node i compared to the true average s_{ave}, so that the MSE of the proposed approach is given by

$$e_{\text{ADQSP}} = \frac{1}{n}\sum_{i\in\mathcal{V}} r_{i,\min}^2. \tag{34}$$

We have that

$$\begin{aligned} r_{i,\min} &= x_i^{(t)} - s_{\text{ave}} \\ &\overset{(a)}{=} \frac{s_i - \sum_{j\in\mathcal{N}_i} B_{i|j}\hat{z}_{i|j}^{(t-1)}}{1+cd_i} - s_{\text{ave}} \\ &\overset{(b)}{=} \frac{s_i - \sum_{j\in\mathcal{N}_i} B_{i|j} z_{i|j}^{(t-1)}}{1+cd_i} - \frac{\sum_{j\in\mathcal{N}_i} B_{i|j} n_{i|j}^{(t-1)}}{1+cd_i} - s_{\text{ave}}, \end{aligned} \tag{35}$$

where (a) uses (21) and (b) uses (20). Since the first term in the right-hand side of (35) equals s_{ave} as $t \to \infty$, we conclude that

$$r_{i,\min} \to -\frac{\sum_{j\in\mathcal{N}_i} B_{i|j} n_{i|j}^{(t-1)}}{1+cd_i} \quad \text{as } t \to \infty.$$

Note that for the special case where $\Delta_{\min} = 0$, we have that $n_{i|j}^{(t)} \to 0$ as $t \to \infty$ and thus $r_{i,\min}^2 \to 0$, hence perfect output accuracy is guaranteed.

B. Individual Privacy

With the adopted quantization scheme, the total collection of information transmitted over the network is $\{z_{i|j}^{(0)}\}_{(i,j)\in\mathcal{E}}, \{\Delta\hat{z}_{i|j}^{(t)}\}_{(i,j)\in\mathcal{E},t\geq 1}$. Of these, only the initialized $\{z_{i|j}^{(0)}\}_{(i,j)\in\mathcal{E}}$ are transmitted over a secure channel. Thus, the eavesdropping adversary has the knowledge of $\{\Delta\hat{z}_{j|k}^{(t)}\}_{(j,k)\in\mathcal{E},t\geq 1}$ The passive adversary has the knowledge of $\{S_j\}_{j\in\mathcal{V}_c} \cup \{Z_{j|k}^{(0)}, \Delta\hat{Z}_{j|k}^{(t)}\}_{(j,k)\in\mathcal{E}_c,t\geq 1}$ and hence combining the knowledge of these gives that the view of an adversary in our proposed algorithm is

$$\mathcal{O}_{\text{ADQSP},\mathcal{V}_c} = \{S_j\}_{j\in\mathcal{V}_c} \cup \{Z_{j|k}^{(0)}\}_{(j,k)\in\mathcal{E}_c} \cup \{\Delta\hat{Z}_{j|k}^{(t)}\}_{(j,k)\in\mathcal{E},t\geq 1}).$$

In what follows we will show that the proposed approach can achieve both SPMC and DP performances under different parameter settings.

C. Proposed Approach Achieves SMPC Performances by Setting $\Delta_{\min} = 0$

We will prove our claim via two main results: 1) the proposed approach obtains similar properties as the SMPC technique, i.e., additive secret sharing; 2) The proposed approach achieves the same performances as the SMPC approach.

We remark that the initialized $z_{i|j}^{(0)}$'s together with $x_i^{(1)}$ can be considered as shares of s_i, similar to the additive secret sharing scheme. In the following, we prove that it also satisfies two key properties of additive secret sharing scheme, similar to Proposition 2.

Proposition 3: (The proposed ADQSP satisfies two properties required for additive secret sharing.) Let $Z_{i|j}^{(0)} \sim \mathcal{N}(0, \sigma_z^2)$ *and let* $x_i^{(1)} = \frac{s_i - \sum_{j\in\mathcal{N}_i} B_{i|j} z_{i|j}^{(0)}}{1+cd_i}$. *Furthermore, let* k *be an element in* $\mathcal{N}_i$ *and denote the variance of* S_i *by* σ_s^2. *Then*

$$\mathrm{I}(S_i; \{Z_{i|j}^{(0)}\}_{j\in\mathcal{N}_i\setminus\{k\}}, X_i^{(1)}) \leq \frac{1}{2}\log(1+\frac{\sigma_s^2}{\sigma_z^2}) \tag{36}$$

$$\mathrm{I}(S_i; \{Z_{i|j}^{(0)}\}_{j\in\mathcal{N}_i}, X_i^{(1)}) = \mathrm{I}(S_i; S_i). \tag{37}$$

For $\sigma_z^2 \to \infty$ *we obtain*

$$\lim_{\sigma_z^2\to\infty} \mathrm{I}(S_i; \{Z_{i|j}^{(0)}\}_{j\in\mathcal{N}_i\setminus\{k\}}, X_i^{(1)}) = 0. \tag{38}$$

Proof: See Appendix G. □

We now proceed to the main results of individual privacy.

Theorem 2: (Upper and lower bound of the information loss of the proposed ADQSP approach when $\Delta_{\min} = 0$.*) Assume that all nodes has at least one corrupt neighbor, the information that the adversaries can infer about an arbitrary honest node* $i \in \mathcal{V}_h$ *is upper bounded by*:

$$\begin{aligned}&\mathrm{I}(S_i; \mathcal{O}_{\mathrm{ADQSP},\mathcal{V}_c})\\ &\leq \mathrm{I}(S_i; \{S_j - \sum_{k\in\mathcal{N}_{j,h}} B_{j|k} Z_{j|k}^{(0)}\}_{j\in\mathcal{V}_{h,1}}, \{Z_{j|k}^{(0)} - Z_{k|j}^{(0)}\}_{j,k\in\mathcal{V}_{h,1}}),\end{aligned} \tag{39}$$

assuming $\sigma_z^2 \to \infty$, *the above becomes*

$$\mathrm{I}(S_i; \mathcal{O}_{\mathrm{ADQSP},\mathcal{V}_c}) \leq \mathrm{I}(S_i; \sum_{j\in\mathcal{V}_{h,1}} S_j). \tag{40}$$

Assuming $t_{\max} \to \infty$, *the information loss is also lower bounded by*:

$$\mathrm{I}(S_i; \mathcal{O}_{\mathrm{ADQSP},\mathcal{V}_c}) \geq I(S_i; \sum_{j\in\mathcal{V}_{h,1}} S_j). \tag{41}$$

Proof: See Appendix I for proof of (39) and (40), Appendix J for proof of (41). □

Overall, we conclude that when $\Delta_{\min} = 0$ the output accuracy and individual privacy of the proposed ADQSP protocol is given by

$$\left(e_{\mathrm{ADQSP}} = 0; \mathrm{I}(S_i; \mathcal{O}_{\mathrm{ADQSP},\mathcal{V}_c}) = \mathrm{I}(S_i; \sum_{j\in\mathcal{V}_{h,1}} S_j).\right) \tag{42}$$

which is identical to the performance of SMPC approach (28).

D. Proposed Approach Achieves Performances of (Relaxed) DP Approaches by Setting $\Delta_{\min} > 0$

DP approach is the worst-case scenario where there are $n-1$ corrupt nodes, i.e., $\mathcal{V}_c = \mathcal{V}\setminus\{i\}$, which implies $\mathcal{N}_{i,h} = \emptyset$ and $\mathcal{G}_i = \{i\}$. We have the following result

Theorem 3: (Information loss of the proposed approach when $\mathcal{V}_c = \mathcal{V}\setminus\{i\}$ *and* $\Delta_{\min} > 0$*) The information loss is given by*

$$\mathrm{I}(S_i; \mathcal{O}_{\mathrm{ADQSP},\mathcal{V}\setminus\{i\}}) = \mathrm{I}(S_i; \{S_i + c_{i,k} N_{k|i}^{(t+1)}\}_{t\geq 0}) \tag{43}$$

where $c_{i,k} = \frac{1+cd_i}{(1-\theta)2cB_{i|k}}$.

Proof: See Appendix K. □

Note that in this case if $\Delta_{\min} = 0$, we have $N_{k|i}^{(t)} \to 0$ thus the above $\mathrm{I}(S_i; \mathcal{O}_{\mathrm{ADQSP},\mathcal{V}\setminus\{i\}}) = \mathrm{I}(S_i; \{S_i + c_{i,k} N_{k|i}^{(t+1)}\}_{t\geq 0}) = \mathrm{I}(S_i; S_i)$ which is maximal, i.e., all the private information is revealed.

Therefore, we should set $\Delta_{\min} > 0$ and the corresponding quantization noise $N_{k|i}^{(t+1)}$ will help to guarantee privacy. By inspecting the output accuracy (34) and individual privacy (43) we can see that increasing $\Delta_{\min}$ will result less accurate output and more privacy guarantee as the quantization noise $n_{i|j}^{(t)}$s at convergence becomes larger. This complies to the privacy-accuracy trade-off of DP discussed in Section V-B. Overall, we conclude that by setting $\Delta_{\min} > 0$, the proposed ADQSP gives privacy guarantees in the presence of $n-1$ corrupt nodes, analogous to DP. Its output accuracy and individual privacy are given by

$$\left(e_{\mathrm{ADQSP}} = \frac{1}{n}\sum_{i\in\mathcal{V}} r_{i,\min}^2; \quad \mathrm{I}(S_i; \mathcal{O}_{\mathrm{ADQSP},\mathcal{V}\setminus\{i\}}) = \mathrm{I}(S_i; \{S_i + c_{i,k} N_{k|i}^{(t+1)}\}_{t\geq 0}).\right) \tag{44}$$

VII. Numerical Results

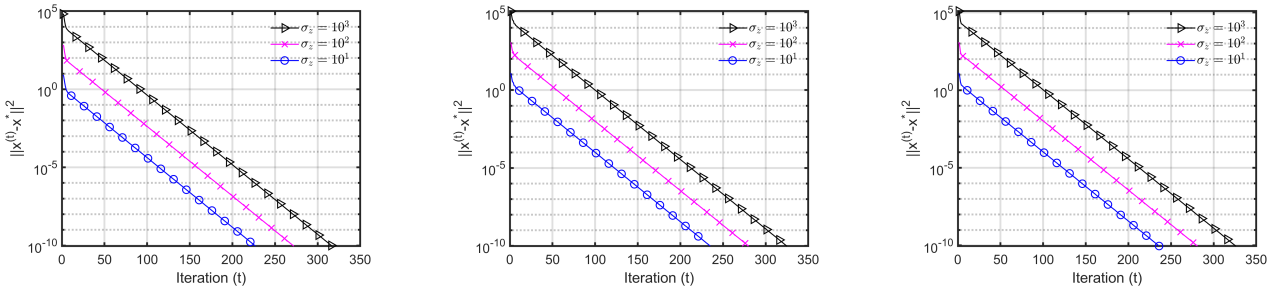
In this section, simulation results will be presented to demonstrate the performance of the proposed approach and its connections to both SMPC and DP.

A. Convergence Behavior of the Proposed Approach

To simulate a distributed network, we simulate a geometric graph with $n = 30$ nodes in a room of size $1 \times 1 \times 1$ meter and the coordinates of each node are randomly generated from uniform distribution within the range of [0, 1]. Every two nodes are neighbors if and only if their distance is within the radius $\sqrt{\frac{2\log(n)}{n}}$, this guarantees that the generated graph will be connected with a high probability [46]. Without loss of generality, all private data $\{s_i\}_{i\in\mathcal{V}}$ are randomly drawn from a Gaussian distribution with unit variance and zero mean. The constant c for controlling the convergence rate is set as 1. The bitrate l is set as 2.

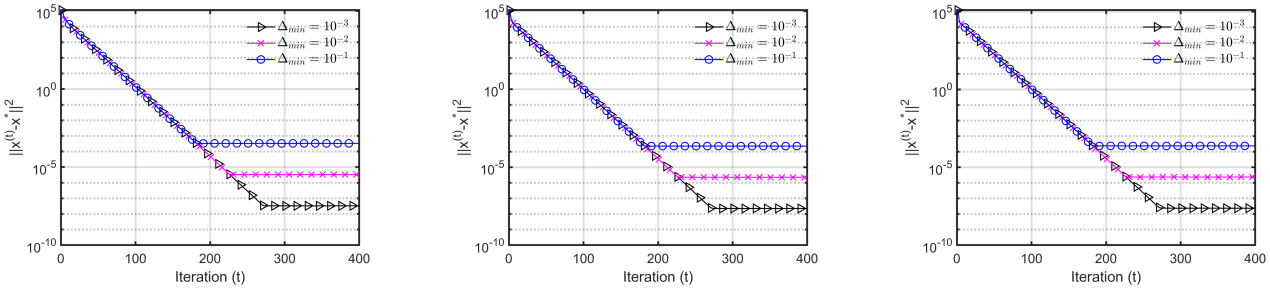
To demonstrate the flexibility and general applicability of the proposed approach, in Fig. 1 and 2 we show its convergence behavior under different parameter settings. Each experiment is averaged over 10^4 times. The mutual information is estimated using the npeet toolbox [47].

1) First, we demonstrate that the proposed approach is applicable to different types of distributed optimizers, i.e., to different choices of $\theta \in [0, 1)$. We take $\theta = 0,\ 0.2,\ 0.5$; note that $\theta = 0$ corresponds to PDMM and $\theta = 0.5$ corresponds to ADMM. As can be seen from Fig. 1 and 2, the convergence behavior is independent of the choice of θ, and our approach can be applied to different distributed optimizers.
2) In Fig. 1 we demonstrate the convergence behavior of the optimization variable by varying the variance of the initialized auxiliary variable, which controls the achieved privacy level (see details below in Fig. 3). Clearly, we can see that the convergence rate is independent of the variance magnitude, as a higher variance only incurs a higher initial error, thus a larger offset.



(a) $\theta = 0$ (b) $\theta = 0.2$ (c) $\theta = 0.5$

Fig. 1. Convergence of the optimization variable in terms of three different variances of the auxiliary variable, i.e., $\sigma_z = 10^3$, $\sigma_z = 10^2$ and $\sigma_z = 10^1$ given three different distributed optimizers: (a) $\theta = 0$ (PDMM), (b) $\theta = 0.2$ and (c) $\theta = 0.5$ (ADMM), wherein $\Delta_{\min} = 0$.



(a) $\theta = 0$ (b) $\theta = 0.2$ (c) $\theta = 0.5$

Fig. 2. Convergence of the optimization variable in terms of three different quantization parameter setting, i.e., $\Delta_{\min} = 10^{-3}$, $\Delta_{\min} = 10^{-2}$ and $\Delta_{\min} = 10^{-1}$ given three different distributed optimizers: (a) $\theta = 0$ (PDMM), (b) $\theta = 0.2$ and (c) $\theta = 0.5$ (ADMM), wherein $\sigma_z = 10^3$.

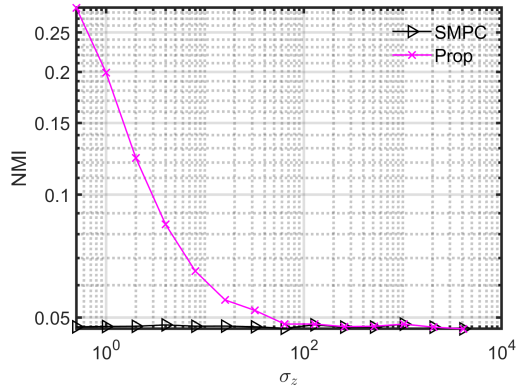


Fig. 3. Individual privacy: normalized mutual information (RHS of (39)) as a function of σ_z using the proposed approach; NMI of $\mathrm{I}(S_i; \sum_{j\in\mathcal{V}_{h,1}} S_j)$ using the existing SMPC approach.

3) In Fig. 2 we demonstrate the convergence behaviors by varying the quantization cell-width $\Delta_{\min}$. We can see that, as expected, the output accuracy is degraded by increasing $\Delta_{\min}$ (in Fig. 5 we will show the privacy leakage becomes less by increasing $\Delta_{\min}$). Hence, the trade-off between privacy and accuracy is controlled by the parameter $\Delta_{\min}$.

B. Connection to Existing SMPC and DP Approaches

We now proceed to consolidate our claims that the proposed approaches can reduce to both SMPC and DP by choosing appropriate parameter settings.

1) SMPC: In Fig. 1 we show that by setting $\Delta_{\min} = 0$ the proposed approach is able to converge to accurate output average result, similar to the results reported in SMPC approach [14], [16]. As for individual privacy, we consider the case where there are only two honest nodes in the network and they are connected to each other. In Fig. 3 we show the achieved privacy level for one honest node of the proposed approach, by taking the normalized mutual information (NMI) on RHS of (39) as a function of the variance σ_z. In addition, we also depict the achieved privacy of the existing SMPC approach, i.e., the normalized mutual information $\mathrm{I}(S_i; \sum_{j\in\mathcal{V}_{h,1}} S_j)$ in the redefined ideal world (8). We see that by increasing the variance σ_z, the proposed approach gets closer to the bound given in SMPC approach. Hence, with Fig. 1 and 3, we validate the claim that the proposed approach can achieve the same performances as SMPC approach when $\Delta_{\min} = 0$.

2) DP: In order to demonstrate that the proposed approach achieves similar privacy to a DP approach by setting $\Delta_{\min} > 0$, we assume that the noise added in DP approach is uniformly distributed over the range $[\frac{-u_r}{2}, \frac{u_r}{2}]$. By inspecting Fig. 4 we can see that by setting $u_r = \Delta_{\min}$, the proposed approach achieves similar output accuracy as the DP approach. Note that by tuning parameters c the constant for controlling the convergence rate and γ the decreasing rate of quantization cell-width, it is possible to achieve a good combination which even has a faster convergence rat compared to the non-quantized case (see [40], [41] for more details). As for individual privacy, let node i be the only honest node and for simplicity we let $c = d_i = 1$ and $\theta = 0$ such that $c_{i,k} = \frac{1+cd_i}{(1-\theta)2cB_{i|k}} = 1$ in (43). In Fig. 5 we plot the NMI of $\mathrm{I}(S_i; \{S_i + c_{i,j} N_{j|i}^{(t+1)}\}_{j\in\mathcal{N}_i})$ as a function of the iteration number t using the proposed approach. For the DP type approach, the NMI is given by $\mathrm{I}(S_i; S_i + R_i)$. From the figure we conclude

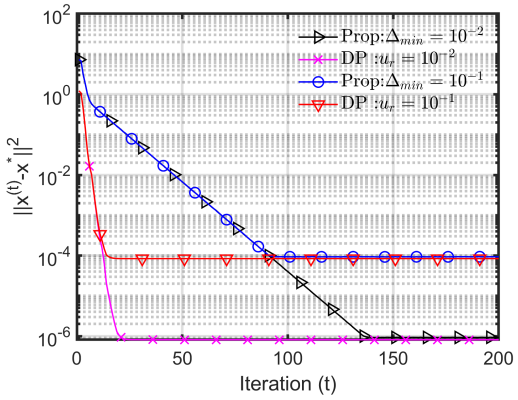


Fig. 4. Output accuracy: MSE of the optimization variable in terms of iteration numbers using the proposed approach and DP approach under two different sets of parameter.

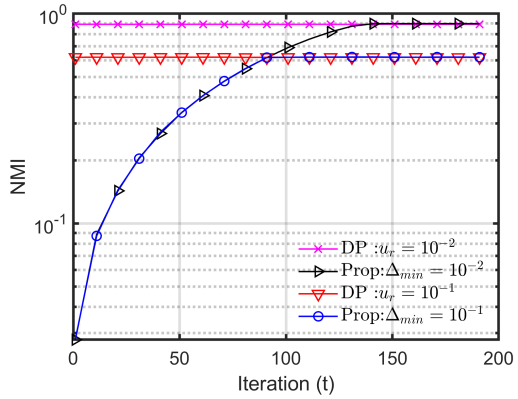


Fig. 5. Individual privacy: NMI as a function of iteration numbers using the proposed approach and DP approach under two different set of parameters.

TABLE I
ABBREVIATIONS

Abbreviation	Full description
SMPC	Secure multiparty computation
DP	Differential privacy
ADQSP	Adaptive differentially quantized subspace perturbation
MSE	Mean squared error
TTP	Trusted third party
LDP	Local differential privacy

that as the iteration grows, $\mathrm{I}(S_i; \{S_i + c_{i,j}N_{j|i}^{(t+1)}\}_{j\in\mathcal{N}_i})$ of the proposed approach can attach to the $\mathrm{I}(S_i; S_i + R_i)$ of DP type approach, which substantiates our theoretical results.

VIII. Conclusion

In this paper, we proposed a novel privacy-preserving distributed average consensus approach called ADQSP. Through a comprehensive information-theoretical privacy analysis, we demonstrate the flexibility and optimality of the proposed approach. Though not directly derived from existing cryptographic tools, it enjoys both the benefits of SMPC and DP techniques and can achieve their performances by controlling the quantization parameter. Experimental results are presented to validate our theoretical analysis.

Appendix A
List of Abbreviations

See Table I.

Appendix B
Broadcast Alternative of Algorithm 1

Algorithm 3 Distributed Optimization for Average Consensus (broadcast)

At each $i \in \mathcal{V}$:
1) Initialize $\{z_{i|j}^{(0)} = 0\}_{j\in\mathcal{N}_i}$;
2) For $t = 0, 1, \ldots, t_{\max} - 1$ do
   a) Compute $x_i^{(t+1)}$ using (10);
   b) Broadcast $x_i^{(t+1)}$ to all $j \in \mathcal{N}_i$;
   c) Compute $\forall j \in \mathcal{N}_i : z_{i|j}^{(t+1)}, z_{j|i}^{(t+1)}$ using (11);
3) Output $x_i^{(t_{\max})}$

Appendix C
Proof of Proposition 1

To explain the main idea we use the case that $k_h = 2$, i.e., the adversary disconnects the honest nodes into two components denoted as a "left" component $\mathcal{L}$ and a "right" component $\mathcal{R}$. Let $\boldsymbol{s}_\mathcal{L}$, $\boldsymbol{s}_\mathcal{R}$ and $\boldsymbol{s}_{\mathcal{V}_c}$ be vectors consisting of the inputs for the left component, the right component, and the corrupt nodes, respectively.

Proof: Let F be the protocol outputting $\sum_{i=1}^n s_i$. The view of the adversary is

$$\mathcal{O}_{\mathrm{F},\mathcal{V}_c} = \{\boldsymbol{s}_{\mathcal{V}_c}, \boldsymbol{r}_{\mathcal{V}_c}, \boldsymbol{m}_\mathcal{L}, \boldsymbol{m}_\mathcal{R}, f(\boldsymbol{s}_\mathcal{L}, \boldsymbol{s}_{\mathcal{V}_c}, \boldsymbol{s}_\mathcal{R})\}, \tag{45}$$

where $\boldsymbol{r}_{\mathcal{V}_c}$ is a vector containing the so-called randomness from the corrupt nodes, $\boldsymbol{m}_\mathcal{L}$ is a vector containing all messages received from nodes in $\mathcal{L}$ and similarly for $\boldsymbol{m}_\mathcal{R}$ in $\mathcal{R}$.

The adversary can simulate a run of the protocol where it takes the actions for the nodes in $\mathcal{R}$. It means that it chooses some inputs and randomness and follow the steps in F, where it uses the messages $\boldsymbol{m}_\mathcal{L}$ when needed in F. If at some point an entry in $\boldsymbol{m}_\mathcal{R}$ differs from the view it will abort the protocol and start over. Since $\boldsymbol{s}_\mathcal{R}$ and $\boldsymbol{r}_\mathcal{R}$ is a valid choice (there might of course be several others) the adversary will succeed at some point meaning that it will find an $\tilde{\boldsymbol{s}}_\mathcal{R}$ and $\tilde{\boldsymbol{r}}_\mathcal{R}$ giving the exact same view as in (45). Since the adversary uses the exact same messages from the nodes in $\mathcal{L}$ as in the real execution of F and the correct output is included in the view we must have $f(\boldsymbol{s}_\mathcal{L}, \boldsymbol{s}_{\mathcal{V}_c}, \boldsymbol{s}_\mathcal{R}) = f(\boldsymbol{s}_\mathcal{L}, \boldsymbol{s}_{\mathcal{V}_c}, \tilde{\boldsymbol{s}}_\mathcal{R})$. Hence, the adversary can determine

$$\sum_{i\in\mathcal{L}} s_i = f(\boldsymbol{s}_\mathcal{L}, \boldsymbol{s}_{\mathcal{V}_c}, \boldsymbol{s}_\mathcal{R}) - \sum_{i\in\mathcal{V}_c} s_i - \sum_{i\in R} \tilde{s}_i$$

When the adversary knows $\sum_{i\in\mathcal{L}} s_i$ it can of course also determine $\sum_{i\in\mathcal{R}} s_i = \sum_{i=1}^n s_i - \sum_{i\in\mathcal{V}_c} s_i - \sum_{i\in\mathcal{L}} s_i$. The above proof can easily be generalized to the case where $k_h > 2$ and that in this case the adversary will learn all the sums of the private data in each component. Hence, the proof is now complete. □

Appendix D
Proof of Proposition 2

Proof: The first equality holds since

$$(r_i^i + \sum_{j\in\mathcal{N}_i} r_i^j) \bmod p = s_i. \tag{46}$$

For the last equality we consider two cases. First assume $k = i$, then clearly $\mathrm{I}(S_i; \{R_i^j\}_{j\in\mathcal{N}_i'\setminus\{k\}}) = 0$ since all the R_i^j are independent of S_i. The last case considers $k \neq i$, and in this case we have that

$$\mathrm{I}(S_i; \{R_i^j\}_{j\in\mathcal{N}_i'\setminus\{k\}}) \overset{(a)}{=} \mathrm{I}(S_i; \{R_i^j\}_{j\in\mathcal{N}_i\setminus\{k\}}, S_i - R_i^k) \overset{(b)}{=} \mathrm{I}(S_i; S_i - R_i^k),$$

where (a) uses (46) and the fact that $\mathrm{I}(X; Y, Z) = \mathrm{I}(X; f(Y, Z))$ if f is a bijective function; (b) follows from independence between $\{S_i, S_i - R_i^k\}$ and $\{R_i^j\}_{j\in\mathcal{N}_i\setminus\{k\}}$. Due to the fact that R_i^k is uniformly distributed in $\mathbb{Z}_p$, the random variable $S_i - R_i^k$ is also uniformly distributed in $\mathbb{Z}_p$ and hence independent of S_i which completes the proof of (25). □

Appendix E
Necessary Result for Proving Theorem 1

Lemma 2: Let $X_1, \ldots X_n$ and $R_1, \ldots R_n$ be independent random variables satisfying $\forall i : \mathrm{I}(X_i; X_i + R_i) = 0$. Then

$$\forall i : \mathrm{I}(X_i; X_1 + R_1, \ldots, X_n + R_n, \sum_{j=1}^{n} R_j) = I(X_i; \sum_{j=1}^{n} X_j).$$

Proof: We first present the following equality:

$$\begin{bmatrix} 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & \cdots & 1 & 1 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & 1 \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix} \begin{bmatrix} X_1 + R_1 \\ X_2 + R_2 \\ \vdots \\ X_n + R_n \\ -\sum_{i=1}^{n} R_i \end{bmatrix} = \begin{bmatrix} \sum_{i=1}^{n} X_i \\ \sum_{i=2}^{n} X_i - R_i \\ \vdots \\ X_n - \sum_{i=1}^{n-1} R_i \\ -\sum_{i=1}^{n} R_i \end{bmatrix} \tag{47}$$

With the above result we have

$$\begin{aligned} &\mathrm{I}(X_i; X_1 + R_1, \ldots, X_n + R_n, \sum_{j=1}^{n} R_j) \\ &= \mathrm{I}(X_i; \sum_{j=1}^{n} X_j, \sum_{j=2}^{n} X_j - R_1, \ldots, X_n - \sum_{j=1}^{n-1} R_j, \sum_{j=1}^{n} R_j) \\ &= I(X_i; \sum_{j=1}^{n} X_j). \end{aligned}$$

where the first equality holds as the linear map in (47) is bijective; by inspecting the linear map we can see that the difference of the k'th and $(k+1)$'th rows in RHS of (47) is $X_k + R_k$, which is independent of all X_is and the k'th row of (47), thus $X_i \to \sum_{j=1}^{n} X_j \to \sum_{j=2}^{n} X_j - R_1 \to \ldots \to X_n - \sum_{j=1}^{n-1} R_i \to \sum_{j=1}^{n} R_j$ forms a Markov chain. Thus, the second equality holds. □

Appendix F
Proof of Theorem 1

Proof: We have that

$$\mathrm{I}(S_i; \mathcal{O}_{\mathrm{SMPC},\mathcal{V}_c}) = \mathrm{I}(S_i; \{S_j\}_{j\in\mathcal{V}_c} \cup \{R_j^k, R_k^j\}_{(j,k)\in\mathcal{E}_c} \cup \{X^{(1)}, X^{(2)}\})$$

as from (27) all $\{X^{(t)}\}_{t\geq 2}$ can be determined using $\{X^{(1)}, X^{(2)}\}$. Furthermore, note that since we initialize $z_{i|j}^{(0)} = 0$ and with the inputs from (26) we have that

$$x_j^{(1)} = \frac{s_j'}{1 + cd_j}$$

$$x_j^{(2)} = \frac{s_j' + 2c(1-\theta)\sum_{k\in\mathcal{V}_j} x_k^{(1)}}{1 + cd_j}$$

from (10) and (11).

Thus, there is a bijection between $\{s_j'\}_{j\in\mathcal{V}}$ and $\boldsymbol{x}^{(1)}$ and furthermore, $\{s_j'\}_{j\in\mathcal{V}}$ is enough for computing $\boldsymbol{x}^{(2)}$. In addition, the corrupt $\{s_j'\}_{j\in\mathcal{V}_c}$ can be computed using $\{s_j\}_{j\in\mathcal{V}_c}$ and $\{r_j^k, r_k^j\}_{(j,k)\in\mathcal{E}_c}$ based on (26). Thus we have

$$\begin{aligned} &\mathrm{I}(S_i; \mathcal{O}_{\mathrm{SMPC},\mathcal{V}_c}) \\ &= \mathrm{I}(S_i; \{S_j\}_{j\in\mathcal{V}_c}, \{R_j^k, R_k^j\}_{(j,k)\in\mathcal{E}_c}, \{S_j'\}_{j\in\mathcal{V}_h}) \\ &\overset{(a)}{=} \mathrm{I}(S_i; \{R_j^k, R_k^j\}_{(j,k)\in\mathcal{E}_c}, \{S_j'\}_{j\in\mathcal{V}_h}) \\ &\overset{(b)}{=} \mathrm{I}(S_i; \{R_j^k, R_k^j\}_{(j,k)\in\mathcal{E}_c}, \{S_j + \sum_{k\in\mathcal{N}_{j,h}} R_k^j - R_j^k\}_{j\in\mathcal{V}_h}) \\ &\overset{(c)}{=} \mathrm{I}(S_i; \{S_j + \sum_{k\in\mathcal{N}_{j,h}} R_k^j - R_j^k\}_{j\in\mathcal{V}_h}) \\ &\overset{(d)}{=} \mathrm{I}(S_i; \{S_j + \sum_{k\in\mathcal{N}_{j,h}} R_k^j - R_j^k\}_{j\in\mathcal{V}_{h,1}}) \\ &\overset{(e)}{=} \mathrm{I}(S_i; \sum_{j\in\mathcal{V}_{h,1}} S_j) \end{aligned}$$

where (a) holds as the term $\{S_j\}_{j\in\mathcal{V}_c}$ is independent of all other terms; (b) uses the fact that $\mathrm{I}(X; Y, Z) = \mathrm{I}(X; f(Y, Z))$ if f is a bijective function, (c) holds as all terms in $\{R_j^k, R_k^j\}_{(j,k)\in\mathcal{E}_c}$ are independent of $\{S_j + \sum_{k\in\mathcal{N}_{j,h}} R_k^j - R_j^k\}_{j\in\mathcal{V}_h}$, and (d) follows from the independence of the different components, and (e) holds as (d) is a special case of Lemma 2 wherein $\sum_{i=1}^{n} R_i = 0$. □

Appendix G
Proof of Proposition 3

Proof: The equality comes immediately as s_i can be determined by $\{z_{i|j}^{(0)}\}_{j\in\mathcal{N}_i}$ and $x_i^{(1)}$ using (10). Now consider the inequality. We have that

$$\begin{aligned} &\mathrm{I}(S_i; \{Z_{i|j}^{(0)}\}_{j\in\mathcal{N}_i\setminus\{k\}}, X_i^{(1)}) \\ &\overset{(a)}{=} \mathrm{I}(S_i; \{Z_{i|j}^{(0)}\}_{j\in\mathcal{N}_i\setminus\{k\}}, S_i - B_{i|k} Z_{i|k}^{(0)}) \\ &\overset{(b)}{=} \mathrm{I}(S_i; S_i - Z_{i|k}^{(0)}) \\ &= h(S_i - Z_{i|k}^{(0)}) - h(Z_{i|k}^{(0)}) \\ &\overset{(c)}{=} h(S_i - Z_{i|k}^{(0)}) - \frac{1}{2}\log(2\pi e\sigma_z^2) \\ &\overset{(d)}{\leq} \log\left(1 + \frac{\sigma_s^2}{\sigma_z^2}\right) \end{aligned}$$

where (a) uses (10) and the fact that $\mathrm{I}(X; Y, Z) = \mathrm{I}(X; f(Y, Z))$ if f is a bijective function. (b) follows as $Z_{i|j}^{(0)}$ is independent of S_i and $Z_{i|k}^{(0)}$ and assuming the constant $B_{i|k} = 1$ (for the case of $B_{i|k} = -1$ the proof is the same.). (c) holds as the entropy of a normal distribution with variance σ^2 is given by $\frac{1}{2}\log(2\pi e\sigma^2)$. (d) follows from the fact that the maximum entropy of a distribution with fixed variance is given by the normal distribution, thus we obtain the above upper bound.

When $\sigma_z^2 \to \infty$, $\frac{\sigma_s^2}{\sigma_z^2} \to 0$ we thus have

$$\lim_{\sigma_z^2\to\infty} \mathrm{I}(S_i; \{Z_{i|j}^{(0)}\}_{j\in\mathcal{N}_i\setminus\{k\}}, X_i^{(1)}) = 0,$$

as mutual information is non-negative. □

APPENDIX H
NECESSARY RESULTS FOR PROVING THEOREM 2

Lemma 3: Let X, R be independent random variables with variance $\sigma_x^2, \sigma_r^2 < \infty$, we have

$$\lim_{\sigma_r^2 \to \infty} \mathrm{I}(X; X+R) = 0, \tag{48}$$

i.e., X is asymptotically independent of $X+R$ if $\sigma_r^2 \to \infty$.

Proof: Let $\gamma = 1/\sigma_r$ and define $R' = \gamma R$. Hence, R' has unit variance. Since mutual information is invariant under scaling, we have $I(X; X+R) = I\left(\gamma X; \gamma X + R'\right)$. As a consequence, we have

$$\begin{aligned}\lim_{\sigma_r^2 \to \infty} I(X; X+R) &= \lim_{\gamma \to 0} I\left(\gamma X; \gamma X + R'\right) \\ &= I\left(0; R'\right) = 0.\end{aligned}$$

□

APPENDIX I
PROOF OF (39) AND (40) IN THEOREM 2

Proof: Consider the difference of two successive $\boldsymbol{x}$-updates (12):

$$\boldsymbol{x}^{(t+1)} - \boldsymbol{x}^{(t)} = -(I + c\boldsymbol{C}^T\boldsymbol{C})^{-1}(\boldsymbol{C}^T \Delta \boldsymbol{z}^{(t)}).$$

Similarly, the difference of two successive $\boldsymbol{z}$ updates in (13) is given by

$$\begin{aligned}\Delta \boldsymbol{z}^{(t+1)} &= \theta \Delta \boldsymbol{z}^{(t)} + (1-\theta)\boldsymbol{P}\Delta \boldsymbol{z}^{(t)} \\ &\quad + 2c(1-\theta)(\boldsymbol{P}\boldsymbol{C}(\boldsymbol{x}^{(t+1)} - \boldsymbol{x}^{(t)})). \\ &= \theta \Delta \boldsymbol{z}^{(t)} + (1-\theta)\boldsymbol{P}\Delta \boldsymbol{z}^{(t)} \\ &\quad - 2c(1-\theta)(I + c\boldsymbol{C}^T\boldsymbol{C})^{-1}(\boldsymbol{P}\boldsymbol{C}\boldsymbol{C}^T \Delta \boldsymbol{z}^{(t)}).\end{aligned} \tag{49}$$

Hence, $\Delta \boldsymbol{z}^{(t+1)}$ can be determined by $\Delta \boldsymbol{z}^{(t)}$.

For an honest node i we have

$$\begin{aligned}&\mathrm{I}(S_i; \mathcal{O}_{\mathrm{ADQSP}, \mathcal{V}_c}) \\ &= \mathrm{I}(S_i; \{S_j\}_{j\in\mathcal{V}_c}, \{Z_{j|k}^{(0)}\}_{(j,k)\in\mathcal{E}_c}, \{\Delta \hat{Z}_{j|k}^{(t)}\}_{(j,k)\in\mathcal{E}, t\geq 1}) \\ &\overset{(a)}{\leq} \mathrm{I}(S_i; \{S_j\}_{j\in\mathcal{V}_c}, \{Z_{j|k}^{(0)}\}_{(j,k)\in\mathcal{E}_c}, \{\Delta Z_{j|k}^{(t)}\}_{(j,k)\in\mathcal{E}, t\geq 1}) \\ &\overset{(b)}{=} \mathrm{I}(S_i; \{S_j\}_{j\in\mathcal{V}_c}, \{Z_{j|k}^{(0)}\}_{(j,k)\in\mathcal{E}_c}, \{\Delta Z_{j|k}^{(1)}\}_{(j,k)\in\mathcal{E}}) \\ &\overset{(c)}{=} \mathrm{I}(S_i; \{S_j\}_{j\in\mathcal{V}_c}, \{Z_{j|k}^{(0)}\}_{(j,k)\in\mathcal{E}_c}, X^{(1)}, \{\Delta Z_{j|k}^{(1)}\}_{(j,k)\in\mathcal{E}_h}) \\ &\overset{(d)}{=} \mathrm{I}(S_i; \{S_j\}_{j\in\mathcal{V}_c}, \{Z_{j|k}^{(0)}\}_{(j,k)\in\mathcal{E}_c}, X^{(1)}, \{Z_{j|k}^{(0)} - Z_{k|j}^{(0)}\}_{(j,k)\in\mathcal{E}_h}) \\ &\overset{(e)}{=} \mathrm{I}(S_i; \{S_j - \sum_{k\in\mathcal{N}_{j,h}} B_{j|k} Z_{j|k}^{(0)}\}_{j\in\mathcal{V}_h}, \{Z_{j|k}^{(0)} - Z_{k|j}^{(0)}\}_{(j,k)\in\mathcal{E}_h}) \\ &\overset{(f)}{=} \mathrm{I}(S_i; \{S_j - \sum_{k\in\mathcal{N}_{j,h}} B_{j|k} Z_{j|k}^{(0)}\}_{j\in\mathcal{V}_{h,1}}, \{Z_{j|k}^{(0)} - Z_{k|j}^{(0)}\}_{j,k\in\mathcal{V}_{h,1}})\end{aligned}$$

where (a) follows from the fact that $\Delta \hat{z}_{j|k}^{(t)}$ is a random function of $\Delta z_{j|k}^{(t)}$ due to quantization, and hence we upper bound the information leakage by replacing $\Delta \hat{z}_{j|k}^{(t)}$ by $\Delta z_{j|k}^{(t)}$. (b) uses the result of (49). Since each node has at least one corrupt neighbor thus $\boldsymbol{x}^{(1)}$ can be determined using $\{z_{j|k}^{(0)}\}_{(j,k)\in\mathcal{E}_c}, \{\Delta z_{j|k}^{(1)}\}_{(j,k)\in\mathcal{E}}$ through (11). In addition, using $\boldsymbol{x}^{(1)}$ and $\{z_{j|k}^{(0)}\}_{(j,k)\in\mathcal{E}_c}$ one can further determine $\{z_{j|k}^{(1)}\}_{(j,k)\in\mathcal{E}_c}$, thus also $\{\Delta z_{j|k}^{(1)}\}_{(j,k)\in\mathcal{E}_c}$. Hence, (c) holds. Since $\Delta z_{i|j}^{(1)} = z_{i|j}^{(1)} - z_{i|j}^{(0)}$, replace $z_{i|j}^{(1)}$ using (11) we thus have

$$\frac{\Delta z_{i|j}^{(1)}}{1-\theta} - 2cB_{j|i}x_j^{(1)} = z_{j|i}^{(0)} - z_{i|j}^{(0)}. \tag{50}$$

Hence, $\{z_{j|i}^{(0)} - z_{i|j}^{(0)}\}_{(i,j)\in\mathcal{E}_h}$ and $\{x_j^{(1)}\}_{j\in\mathcal{V}_h}$ can determine $\{\Delta z_{i|j}^{(1)}\}_{(i,j)\in\mathcal{E}_h}$, thus (d) holds. In addition, from (10) we have

$$(1+cd_i)x_i^{(1)} + \sum_{j\in\mathcal{N}_{i,c}} B_{i|j} z_{i|j}^{(0)} = s_i - \sum_{j\in\mathcal{N}_{i,h}} B_{i|j} z_{i|j}^{(0)},$$

which again all term in the LHS is known to the adversaries, and hence we obtain (e). For (e) we also remove $x_j^{(1)}$ for corrupt j's since they can be computed from $\{S_j\}_{j\in\mathcal{V}_c}, \{Z_{j|k}^{(0)}\}_{(j,k)\in\mathcal{E}_c}$ and after removal of this $\{Z_{j|k}^{(0)}\}_{(j,k)\in\mathcal{E}_c}$ is independent of the rest and can be removed. (f) follows by the independence of the different components. Hence, the proof of (39) is complete.

If $\sigma_z^2 \to \infty$, based on Lemma 3 we have $i \in \mathcal{V}_{h,1}$: $\lim_{\sigma_z^2\to\infty} \mathrm{I}(S_i; S_i - \sum_{k\in\mathcal{N}_{i,h}} B_{i|k} Z_{i|k}^{(0)}) = 0$, i.e., the private data S_i is asymptotically independent of $S_i - \sum_{k\in\mathcal{N}_{i,h}} B_{i|k} Z_{i|k}^{(0)}$. Thus, the independence condition required in Lemma 2 is satisfied, the proof follows similarly, we thus have,

$$\begin{aligned}&\mathrm{I}(S_i; \{S_j - \sum_{k\in\mathcal{N}_{j,h}} B_{j|k} Z_{j|k}^{(0)}\}_{j\in\mathcal{V}_{h,1}}, \{Z_{j|k}^{(0)} - Z_{k|j}^{(0)}\}_{j,k\in\mathcal{V}_{h,1}}) \\ &= \mathrm{I}(S_i; \sum_{j\in\mathcal{V}_{h,1}} S_j).\end{aligned}$$

Hence, proof of (40) is complete. □

APPENDIX J
PROOF OF (41) IN THEOREM 2

Proof: We first derive some equalities which will be used in the proof later. Since $\Delta z_{j|i}^{(t+1)} = z_{j|i}^{(t+1)} - \hat{z}_{j|i}^{(t)} = \Delta \hat{z}_{j|i}^{(t+1)} - n_{j|i}^{(t+1)}$, replace $z_{j|i}^{(t+1)}$ using (22) we thus have $\forall t \geq 1$

$$\frac{\Delta \hat{z}_{j|i}^{(t+1)} - n_{j|i}^{(t+1)}}{1-\theta} - 2cB_{i|j}x_i^{(t+1)} = \hat{z}_{i|j}^{(t)} - \hat{z}_{j|i}^{(t)}. \tag{51}$$

Thus, for the corrupt neighbor $k \in \mathcal{N}_{i,c}$ the above becomes

$$x_i^{(t+1)} + \frac{n_{k|i}^{(t+1)}}{2cB_{i|k}(1-\theta)} = \frac{-\hat{z}_{i|k}^{(t)} + \hat{z}_{k|i}^{(t)}}{2cB_{i|k}} + \frac{\Delta \hat{z}_{k|i}^{(t+1)}}{2cB_{i|k}(1-\theta)}. \tag{52}$$

For the honest neighbor $j \in \mathcal{N}_{i,h}$, using (19) the above (51) becomes

$$\begin{aligned}&x_i^{(t+1)} + \frac{n_{j|i}^{(t+1)}}{2cB_{i|j}(1-\theta)} + \frac{z_{i|j}^{(0)} - z_{j|i}^{(0)}}{2cB_{i|j}} \\ &= \frac{-\sum_{\tau=1}^{(t)} \Delta \hat{z}_{i|j}^{(\tau)} + \sum_{\tau=1}^{(t)} \Delta \hat{z}_{j|i}^{(\tau)}}{2cB_{i|j}} + \frac{\Delta \hat{z}_{j|i}^{(t+1)}}{2cB_{i|j}(1-\theta)}.\end{aligned} \tag{53}$$

Using (19), (21) can be written as

$$\begin{aligned}&s_i - \sum_{j\in\mathcal{N}_{i,h}} B_{i|j} z_{i|j}^{(0)} - (1+cd_i)x_i^{(t+1)} \\ &= \sum_{j\in\mathcal{N}_{i,h}} B_{i|j} (\sum_{\tau=1}^{t} \Delta \hat{z}_{i|j}^{(\tau)}) + \sum_{k\in\mathcal{N}_{i,c}} B_{i|k} \hat{z}_{i|k}^{(t)},\end{aligned} \tag{54}$$

Note that, all terms in the RHS of the above equations are known by the adversary, i.e., included in $\mathcal{O}_{\text{ADQSP},\mathcal{V}_c}$.

As a consequence, take the difference of the LHS of (53) and (52) and scale up by $2c$ we have

$$\frac{n_{j|i}^{(t+1)}}{B_{i|j}(1-\theta)}+\frac{z_{i|j}^{(0)}-z_{j|i}^{(0)}}{B_{i|j}}-\frac{n_{k|i}^{(t+1)}}{B_{i|k}(1-\theta)} \tag{55}$$

In addition, first multiple $(1+cd_i)$ with the LHS of (52) and add to LHS of (54) we have

$$s_i-\sum_{j\in\mathcal{N}_{i,h}} B_{i|j}z_{i|j}^{(0)}+c_{i,k}N_{k|i}^{(t+1)}, \tag{56}$$

recall $c_{i,k}=\frac{(1+cd_i)}{2cB_{i|k}(1-\theta)}$.

With the above results we thus have

$$\begin{aligned}
&\mathrm{I}(S_i;\mathcal{O}_{\text{ADQSP},\mathcal{V}_c})\\
&\overset{(a)}{=}\mathrm{I}\Big(S_i;\{S_j\}_{j\in\mathcal{V}_c},\{Z_{j|k}^{(0)}\}_{(j,k)\in\mathcal{E}_c},\{\Delta\hat{Z}_{j|k}^{(t)}\}_{(j,k)\in\mathcal{E},t\geq 1},\\
&\quad\{\frac{N_{j|i}^{(t+1)}}{B_{i|j}(1-\theta)}+\frac{Z_{i|j}^{(0)}-Z_{j|i}^{(0)}}{B_{i|j}}\\
&\quad-\frac{N_{k|i}^{(t+1)}}{B_{i|k}(1-\theta)}\}_{i\in\mathcal{V}_h,j\in\mathcal{N}_{i,h},k\in\mathcal{N}_{i,c},t\geq 0},\\
&\quad\{S_i-\sum_{j\in\mathcal{N}_{i,h}}B_{i|j}Z_{i|j}^{(0)}+c_{i,k}N_{k|i}^{(t+1)}\}_{i\in\mathcal{V}_h,k\in\mathcal{N}_{i,c},t\geq 0}\Big)\\
&\overset{(b)}{\geq}\mathrm{I}\Big(S_i;\{\frac{N_{j|i}^{(t+1)}}{B_{i|j}(1-\theta)}+\frac{Z_{i|j}^{(0)}-Z_{j|i}^{(0)}}{B_{i|j}}\\
&\quad-\frac{N_{k|i}^{(t+1)}}{B_{i|k}(1-\theta)}\}_{i\in\mathcal{V}_{h,1},j\in\mathcal{N}_{i,h},k\in\mathcal{N}_{i,c},t\geq 0},\\
&\quad\{S_i-\sum_{j\in\mathcal{N}_{i,h}}B_{i|j}Z_{i|j}^{(0)}+c_{i,k}N_{k|i}^{(t+1)}\}_{i\in\mathcal{V}_{h,1},k\in\mathcal{N}_{i,c},t\geq 0}\Big)\\
&\overset{(c)}{\geq}\mathrm{I}\Big(S_i;\{\sum_{j\in\mathcal{V}_{h,1}}S_j-\sum_{j,l\in\mathcal{V}_{h,1}}B_{l|j}(N_{l|j}^{(t+1)}-N_{j|l}^{(t+1)})\\
&\quad+\sum_{j\in\mathcal{V}_{h,1},k\in\mathcal{N}_{j,c}}c_{j,k}N_{k|j}^{(t+1)}\}_{t\geq 0}\Big)\\
&\overset{(d)}{\geq}\mathrm{I}\Big(S_i;\sum_{j\in\mathcal{V}_{h,1}}S_j-\sum_{j,l\in\mathcal{V}_{h,1}}B_{i|j}(N_{l|j}^{(t_{\max})}-N_{j|l}^{(t_{\max})})\\
&\quad+\sum_{j\in\mathcal{V}_{h,1},k\in\mathcal{N}_{j,c}}c_{j,k}N_{k|j}^{(t_{\max})}\Big),
\end{aligned}$$

where (a) uses the fact that (55) and (56) can be computed by the knowledge of the adversary. (b) holds by removing the first three terms and consider only the honest component $\mathcal{V}_{h,1}$. (c) holds by making a linear combination of the terms in (b) where the coefficients are $\frac{1}{2|\mathcal{N}_{i,c}|}$ for the first terms and $\frac{1}{|\mathcal{N}_{i,c}|}$ for the remaining terms. (d) holds because we consider only the last iteration $t_{\max}$.

Remark that if $\Delta_{\min}=0$ then $N_{i|j}^{(t_{\max})}$ will converge almost surely to 0 when $t_{\max}\to\infty$. Hence in the limit we have

$$\mathrm{I}(S_i;\mathcal{O}_{\text{ADQSP},\mathcal{V}_c})\geq\mathrm{I}(S_i;\sum_{j\in\mathcal{V}_{h,1}}S_j).$$

Hence, the proof of (41) is complete. □

Appendix K
Proof of Theorem 3

Proof: We first present the following equality result: similar to (13), consider the difference of two successive z updates in (22):

$$\begin{aligned}
&\Delta\hat{z}_{j|i}^{(t+1)}+n_{j|i}^{(t+1)}-n_{j|i}^{(t)}\\
&=\theta\Delta\hat{z}_{j|i}^{(t)}+(1-\theta)\Delta\hat{z}_{i|j}^{(t)}-\frac{2c(1-\theta)B_{i|j}}{1+cd_i}\sum_{k\in\mathcal{N}_i}B_{i|k}\Delta\hat{z}_{i|k}^{(t)}.
\end{aligned} \tag{57}$$

Hence, $\Delta\hat{z}_{j|i}^{(t+1)}$ can be determined by the difference of quantization noise over successive iterations $n_{j|i}^{(t+1)}-n_{j|i}^{(t)}$ and $\Delta\hat{z}_{j|i}^{(t)}$ and $\Delta\hat{z}_{i|j}^{(t)}$ in the previous iteration.

As for $\Delta\hat{z}_{j|i}^{(1)}$ in the first iteration we have

$$\begin{aligned}
\Delta\hat{z}_{j|i}^{(1)}&\overset{(a)}{=}z_{j|i}^{(1)}-z_{j|i}^{(0)}+n_{j|i}^{(1)}\\
&\overset{(b)}{=}(1-\theta)(z_{i|j}^{(0)}-z_{j|i}^{(0)})\\
&\quad+\frac{1}{c_{i,j}}(s_i+c_{i,j}n_{j|i}^{(1)}-\sum_{k\in\mathcal{N}_i}B_{i|k}z_{i|k}^{(0)}),
\end{aligned} \tag{58}$$

where (a) uses (18) and (20); (b) replaces $z_{j|i}^{(1)}$ using (10) and (11).

We start our proof similar to the proof in Appendix J. However, since $\mathcal{V}_c=\mathcal{V}\setminus\{i\}$, $\mathcal{V}_h=\{i\}$ and $\mathcal{N}_{i,h}=\emptyset$ we do not have any honest neighbors and hence we are not adding (55). Thus the equality (a) in the proof of Appendix J becomes the first equality below:

$$\begin{aligned}
&\mathrm{I}(S_i;\mathcal{O}_{\text{ADQSP},\mathcal{V}\setminus\{i\}})\\
&=\mathrm{I}\Big(S_i;\{S_j\}_{j\in\mathcal{V}\setminus\{i\}},\{Z_{j|k}^{(0)},\Delta\hat{Z}_{j|k}^{(t)}\}_{(j,k)\in\mathcal{E},t\geq 1},\\
&\quad\{S_i+c_{i,k}N_{k|i}^{(t+1)}\}_{k\in\mathcal{N}_i,t\geq 0}\Big)\\
&\overset{(a)}{=}\mathrm{I}\Big(S_i;\{S_j\}_{j\in\mathcal{V}\setminus\{i\}},\{Z_{j|k}^{(0)},\Delta\hat{Z}_{j|k}^{(t)}\}_{(j,k)\in\mathcal{E},t\geq 1},\\
&\quad\{N_{k|i}^{(t+1)}-N_{k|i}^{(t)}\}_{k\in\mathcal{N}_i,t\geq 1},\{S_i+c_{i,k}N_{k|i}^{(t+1)}\}_{k\in\mathcal{N}_i,t\geq 0}\Big)\\
&\overset{(b)}{=}\mathrm{I}\Big(S_i;\{S_j\}_{j\in\mathcal{V}\setminus\{i\}},\{Z_{j|k}^{(0)},\Delta\hat{Z}_{j|k}^{(1)}\}_{(j,k)\in\mathcal{E}},\\
&\quad\{N_{k|i}^{(t+1)}-N_{k|i}^{(t)}\}_{k\in\mathcal{N}_i,t\geq 1},\{S_i+c_{i,k}N_{k|i}^{(t+1)}\}_{k\in\mathcal{N}_i,t\geq 0}\Big)\\
&\overset{(c)}{=}\mathrm{I}\Big(S_i;\{S_j\}_{j\in\mathcal{V}\setminus\{i\}},\{Z_{j|k}^{(0)}\}_{(j,k)\in\mathcal{E}},\\
&\quad\{N_{k|i}^{(t+1)}-N_{k|i}^{(t)}\}_{k\in\mathcal{N}_i,t\geq 1},\{S_i+c_{i,k}N_{k|i}^{(t+1)}\}_{k\in\mathcal{N}_i,t\geq 0}\Big)\\
&\overset{(d)}{=}\mathrm{I}\Big(S_i;\{N_{k|i}^{(t+1)}-N_{k|i}^{(t)}\}_{k\in\mathcal{N}_i,t\geq 1},\{S_i+c_{i,k}N_{k|i}^{(t+1)}\}_{k\in\mathcal{N}_i,t\geq 1}\Big)\\
&\overset{(e)}{=}\mathrm{I}\Big(S_i;\{S_i+c_{i,k}N_{k|i}^{(t+1)}\}_{k\in\mathcal{N}_i,t\geq 1}\Big)
\end{aligned}$$

where (a) follows as $\{N_{k|i}^{(t+1)}-N_{k|i}^{(t)}\}_{k\in\mathcal{N}_i,t\geq 1}$ can be computed by taking the difference of the last term over successive iterations. (b) holds as based on (57), all $\{\Delta\hat{Z}_{j|k}^{(t)}\}_{(j,k)\in\mathcal{E},t\geq 2}$ can be computed using $\{N_{k|i}^{(t+1)}-N_{k|i}^{(t)}\}_{k\in\mathcal{N}_i,t\geq 1}$ and $\{S_j\}_{j\in\mathcal{V}\setminus\{i\}},\{Z_{j|k}^{(0)},\Delta\hat{Z}_{j|k}^{(1)}\}_{(j,k)\in\mathcal{E},t\geq 1}$. (c) holds as $\{\Delta\hat{Z}_{j|k}^{(1)}\}_{(j,k)\in\mathcal{E}}$ can be computed using the other terms based on (58). (d) holds as $\{S_j\}_{j\in\mathcal{V}\setminus\{i\}},\{Z_{j|k}^{(0)}\}_{(j,k)\in\mathcal{E}}$ are independent of the rest two terms. (e) holds as $\{N_{k|i}^{(t+1)}-N_{k|i}^{(t)}\}_{k\in\mathcal{N}_i,t\geq 1}$ can

be determined by $\{S_i + c_{i,k} N_{k|i}^{(t+1)}\}_{k\in\mathcal{N}_i, t\geq 1}$. Hence, the proof is complete. □

REFERENCES

[1] J. Poushter, "Smartphone ownership and Internet usage continues to climb in emerging economies," *Pew Res. Center*, vol. 22, pp. 1–44, 2016.

[2] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proc. IEEE*, vol. 95, no. 1, pp. 215–233, Jan. 2007.

[3] J. N. Tsitsiklis, "Problems in decentralized decision making and computation," Ph.D. dissertation, Massachusetts Inst. Technol., Cambridge, MA, USA, 1984.

[4] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Process. Mag.*, vol. 37, no. 3, pp. 50–60, May 2020.

[5] R. C. Hendriks, Z. Erkin, and T. Gerkmann, "Privacy-preserving distributed speech enhancement forwireless sensor networks by processing in the encrypted domain," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, May 2013, pp. 7005–7009.

[6] M. H. Ruan, M. Ahmad, and Y. Q. Wang, "Secure and privacy-preserving average consensus," in *Proc. Workshop Cyber Phys. Syst. Secur. Privacy*, 2017, pp. 123–129.

[7] P. Braca, R. Lazzeretti, S. Marano, and V. Matta, "Learning with privacy in consensus + obfuscation," *IEEE Signal Process. Lett.*, vol. 23, no. 9, pp. 1174–1178, Sep. 2016.

[8] M. T. Hale and M. Egerstedty, "Differentially private cloud-based multi-agent optimization with constraints," in *Proc. Amer. Control Conf. (ACC)*, Jul. 2015, pp. 1235–1240.

[9] M. T. Hale and M. Egerstedt, "Cloud-enabled differentially private multiagent optimization with constraints," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 4, pp. 1693–1706, Dec. 2018.

[10] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design," *Automatica*, vol. 81, pp. 221–231, Jul. 2017.

[11] M. Kefayati, M. S. Talebi, B. H. Khalaj, and H. R. Rabiee, "Secure consensus averaging in sensor networks using random offsets," in *Proc. IEEE Int. Conf. Telecommun. Malaysia Int. Conf. Commun.*, 2007, pp. 556–560.

[12] Z. Huang, S. Mitra, and G. Dullerud, "Differentially private iterative synchronous consensus," in *Proc. ACM Workshop Privacy Electron. Soc.*, Oct. 2012, pp. 81–90.

[13] Y. Guo and Y. Gong, "Practical collaborative learning for crowdsensing in the Internet of Things with differential privacy," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, May 2018, pp. 1–9.

[14] N. Gupta, J. Katz, and N. Chopra, "Privacy in distributed average consensus," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 9515–9520, 2017.

[15] N. Gupta, J. Kat, and N. Chopra, "Statistical privacy in distributed average consensus on bounded real inputs," in *Proc. Amer. Control Conf. (ACC)*, Jul. 2019, pp. 1836–1841.

[16] Q. Li, I. Cascudo, and M. G. Christensen, "Privacy-preserving distributed average consensus based on additive secret sharing," in *Proc. 27th Eur. Signal Process. Conf. (EUSIPCO)*, Sep. 2019, pp. 1–5.

[17] Q. Li and M. G. Christensen, "A privacy-preserving asynchronous averaging algorithm based on Shamir's secret sharing," in *Proc. 27th Eur. Signal Process. Conf. (EUSIPCO)*, Sep. 2019, pp. 1–5.

[18] Q. Li, R. Heusdens, and M. G. Christensen, "Convex optimisation-based privacy-preserving distributed average consensus in wireless sensor networks," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, May 2020, pp. 5895–5899.

[19] Q. Li, R. Heusdens, and M. G. Christensen, "Privacy-preserving distributed optimization via subspace perturbation: A general framework," *IEEE Trans. Signal Process.*, vol. 68, pp. 5983–5996, 2020.

[20] N. E. Manitara and C. N. Hadjicostis, "Privacy-preserving asymptotic average consensus," in *Proc. Eur. Control Conf. (ECC)*, Jul. 2013, pp. 760–765.

[21] Y. Mo and R. M. Murray, "Privacy preserving average consensus," *IEEE Trans. Autom. Control*, vol. 62, no. 2, pp. 753–765, Feb. 2017.

[22] J. He, L. Cai, C. Zhao, P. Cheng, and X. Guan, "Privacy-preserving average consensus: Privacy analysis and algorithm design," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 5, no. 1, pp. 127–138, Mar. 2019.

[23] Y. Xiong and Z. Li, "Privacy-preserved average consensus algorithms with edge-based additive perturbations," *Automatica*, vol. 140, Jun. 2022, Art. no. 110223.

[24] Y. Zhou and S. Pu, "Private and accurate decentralized optimization via encrypted and structured functional perturbation," *IEEE Control Syst. Lett.*, vol. 7, pp. 1339–1344, 2023.

[25] Q. Li, J. S. Gundersen, R. Heusdens, and M. G. Christensen, "Privacy-preserving distributed processing: Metrics, bounds and algorithms," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2090–2103, 2021.

[26] C. Dwork, "Differential privacy," in *Proc. Int. Colloq. Automata, Lang. Program. (ICALP)*, 2006, pp. 1–12.

[27] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Proc. Theory Cryptogr. Conf.*, 2006, pp. 265–284.

[28] Q. Li, M. Lopuhaä-Zwakenberg, R. Heusdens, and M. G. Christensen, "Two for the price of one: Communication efficient and privacy-preserving distributed average consensus using quantization," in *Proc. 30th Eur. Signal Process. Conf. (EUSIPCO)*, Aug. 2022, pp. 2166–2170.

[29] T. M. Cover and J. A. Tomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 2012.

[30] Y. Bu, S. Zou, and V. V. Veeravalli, "Tightening mutual information-based bounds on generalization error," *IEEE J. Sel. Areas Inf. Theory*, vol. 1, no. 1, pp. 121–130, May 2020.

[31] P. Cuff and L. Yu, "Differential privacy as a mutual information constraint," in *Proc. 23rd ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 43–54.

[32] G. Barthe and B. Kopf, "Information-theoretic bounds for differentially private mechanisms," in *Proc. IEEE 24th Comput. Secur. Found. Symp.*, Jun. 2011, pp. 191–204.

[33] M. Gotz, A. Machanavajjhala, G. Wang, X. Xiao, and J. Gehrke, "Publishing search logs—A comparative study of privacy guarantees," *IEEE Trans. Knowl. Data Eng.*, vol. 24, no. 3, pp. 520–532, Mar. 2012.

[34] A. Beimel, "On private computation in incomplete networks," in *Structural Information and Communication Complexity*, Berlin, Germany: Springer, 2005, pp. 18–33.

[35] Q. Li, R. Heusdens, and M. G. Christensen, "Communication efficient privacy-preserving distributed optimization using adaptive differential quantization," *Signal Process.*, vol. 194, May 2022, Art. no. 108456.

[36] S. Boyd, "Distributed optimization and statistical learning via the alternating direction method of multipliers," *Found. Trends Mach. Learn.*, vol. 3, no. 1, pp. 1–122, 2010.

[37] G. Zhang and R. Heusdens, "Distributed optimization using the primal-dual method of multipliers," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 4, no. 1, pp. 173–187, Mar. 2018.

[38] T. W. Sherson, R. Heusdens, and W. B. Kleijn, "Derivation and analysis of the primal-dual method of multipliers based on monotone operator theory," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 5, no. 2, pp. 334–347, Jun. 2019.

[39] E. K. Ryu and S. Boyd, "Primer on monotone operator methods," *Appl. Comput. Math*, vol. 15, no. 1, pp. 3–43, 2016.

[40] D. H. M. Schellekens, T. Sherson, and R. Heusdens, "Quantisation effects in PDMM: A first study for synchronous distributed averaging," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Mar. 2017, pp. 4237–4241.

[41] J. A. G. Jonkman, T. Sherson, and R. Heusdens, "Quantisation effects in distributed optimisation," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Apr. 2018, pp. 3649–3653.

[42] L. Schuchman, "Dither signals and their effect on quantization noise," *IEEE Trans. Commun.*, vol. COM-12, no. 4, pp. 162–165, Dec. 1964.

[43] D. Dolev, C. Dwork, O. Waarts, and M. Yung, "Perfectly secure message transmission," *J. ACM*, vol. 40, no. 1, pp. 17–47, Jan. 1993.

[44] R. Cramer, I. B. Damgård, and J. B. Nielsen, *Secure Multiparty Computation and Secret Sharing*. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2015, doi: 10.1017/CBO9781107337756.

[45] S. P. Kasiviswanathan, H. K. Lee, K. Nissim, S. Raskhodnikova, and A. Smith, "What can we learn privately?" *SIAM J. Comput.*, vol. 40, no. 3, pp. 793–826, Jan. 2011.

[46] J. Dall and M. Christensen, "Random geometric graphs," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 66, no. 1, 2002, Art. no. 016121.

[47] G. Ver Steeg. (2000). *Non-Parametric Entropy Estimation Toolbox (NPEET)*. [Online]. Available: https://github.com/gregversteeg/NPEET