Privacy-Preserving Distributed Maximum Likelihood Estimation via State Decomposition

Parth Paritosh, *Member, IEEE,* and Lance Kaplan, *Fellow, IEEE*

***Abstract*—This study deals with collaborative yet privacy-preserving estimation algorithms in a sensor network. In particular, the sensing agents sample from Gaussian densities with heterogeneous private covariances, and aim to cooperatively compute the maximum likelihood estimate (MLE) of the common mean. To maintain accuracy and minimize computational load, we adopt the state decomposition (SD) approach that splits the estimated variable into private and public components. First, we design a privacy attack model (PAM) to show that the existing SD-based privacy-preserving algorithm for dynamic consensus does not remain simultaneously private and converge with convergent inputs. To address this issue, we modify the existing continuous-time distributed SD algorithm for discrete-time networked updates with an additional initial mixing step and bounded inputs. When true covariances are known, the algorithm computes the mean MLE estimate while keeping the data and covariances private, and converges at the same rate as the non-private, centralized setting. When agents are estimating covariances locally, the algorithm estimates the mean MLE while keeping the local covariances private and maintains the same convergence rate as the local estimates. The rate compared to local estimates depends on the network structure. In simulations, the estimates from the proposed algorithms converge faster than the sample averaging and standard consensus methods.**

I. Introduction

We consider a network of sensing agents collaborating to estimate a common parameter without leaking any local data or individual characteristics such as detection thresholds, filtering constants, calibration profiles or aggregate statistics [1]. The agents may aim to infer the maximum likelihood estimate (MLE) of an unknown parameter via estimation [2], [3], a target's position via localization [4], [5], or model weights via optimization [6], [7]. The knowledge of individual sensor characteristics enables efficient second order estimation of parameters such as occupancy and comfort uncertainties in a smart building, and platform detection and persistent monitoring in integrated radar defense setting. Their disclosure may reveal sensitive information about the sensor's fidelity and even its operational environment. These characteristics are either known apriori, or estimated in real-time for complex deployments. To account for these issues, several versions of distributed estimation and learning algorithms were developed to preserve the data privacy. But their focus on data ignores the need of privacy for intermediate statistics and operational model settings. We next discuss such algorithms in the context of estimation accuracy, privacy of underlying data and statistics, and computational and communication complexity.

In standard consensus algorithms [8], agents share their estimates [9], [10] directly with neighbors at each time, rendering them unsuitable for privacy-sensitive applications. Therefore, privacy-preserving estimation algorithms have been designed in networked settings. These algorithms [11] can be grouped broadly into two categories, based on underlying privacy mechanism of encryption and signal distortions. Encryption-based techniques use public and private keys to ensure that only the intended recipient reads the transmitted message. Homomorphic encryption [12] is a specialized approach that encrypts data for addition or multiplication at other nodes with a secret key. Although the transmitted messages are accurate, the associated processing costs are prohibitive [13], especially in online settings. Secure multiparty computation is a related technique that splits secret values into several components, a multiple of which needs to be collected for decryption. With lower processing costs than encryption, it has been used to perform private aggregation [14], [15] in distributed algorithms. Still, the associated communication costs remain high due to the need to collect sufficient components for decryption at each iteration.

Among signal-distorting techniques, differential privacy-based algorithms [16], [17] obfuscate shared messages by adding random or summable noise [18], [19] at each agent. Due to the added noise, these algorithms either trade off accuracy for noise or rely on additional coordination. Finally, the state decomposition (SD) methods [20] split the estimates and corresponding inputs into public and private components. This avoids the costly encryption methods while maintaining accurate convergence, but may need additional adaptations for specific applications. These SD-based methods have been adapted to distributed optimization [21] and formation control [22], and in this paper, we extend this method towards private MLE estimation in a network.

Specifically, this work deals with a group of sensors sampling data from individual Gaussian distributions defined via a common mean but distinct covariances. The sensing agents collaborate to find the maximum likelihood estimate (MLE) of the mean. It is an unbiased estimator weighing the observations with the inverse sensor covariances in this distributed setting, leading to a minimum variance estimator. Unbiased but private minimum variance estimation is crucial in problems such as survey design [23], spatial crowdsourcing [24], sensor fusion [25], [26], distributed controls [27], and smart grids [28].

In addition, when the sensor covariances are private but unknown, the agents estimate them locally and collaborate over the network to estimate their time-varying averages to

The authors are with the U.S. Army Combat Capabilities Development Command Army Research Laboratory (DEVCOM ARL), Adelphi, Maryland, pparitos@ucsd.edu, lance.m.kaplan.civ@army.mil. Research was sponsored by the Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF24-2-0101. This paper has supplementary downloadable material containing probabilistic convergence analyses available at http://ieeexplore.ieee.org., provided by the author.

Manuscript received May 31, 2025.

compute MLE. This requires reliable and private consensus over time-varying but convergent signals. *Dynamic Average Consensus* (DAC) [29], [30] is a class of algorithms designed for distributed tracking of the average of time-varying signals at each node in a network, with applications to path planning, state estimation and resource allocation. Even though algorithms such as DAC do not share raw inputs, researchers have designed observers to extract the original inputs [22]. While the convergence of estimates in standard DAC algorithms is guaranteed for convergent inputs [31], we show that the same is not guaranteed in the case of its privacy preserving version based on state decomposition. Therefore, this paper extends the state decomposition approach that allows a fully distributed estimation in a recursive manner, minimal communication costs and leads to accurate estimates.

Our preliminary work in [32] presents SD for private estimation of convergent vector signals. This work augments the algorithm to estimate MLE mean requiring averages of matrices and vectors, and proves the characteristics of attack model, privacy and convergence. In contrast to convergence rate determined by local signals, this work establishes consensus based improvements matching centralized setting in case of known covariances and empirically studies the impact of privacy preservation on convergence.

Statement of Contributions: In this work, we design private dynamic consensus algorithms to compute maximum likelihood estimators while maintaining the privacy of the local samples and covariances. The primary contributions of this work are: (a) *Privacy attack model (PAM) for convergent inputs:* We show that the extant private-preserving DAC tracker [22] is not appropriate for estimation by designing an eavesdropping PAM that uses publicly available variables to recover the convergent agent inputs. (b) *Data and statistic privacy for convergent inputs:* We present a distributed estimation algorithm to accurately estimate the average information matrix and subsequently the average information mean, while guaranteeing privacy for local inputs, even if they are a convergent statistic. (c) *Convergence guarantees for privacy-preserving estimates*: When agents know their true covariances, average information matrix estimates converge at a geometric rate, matching static consensus algorithm, and the mean MLE convergence matches the centralized rate. With locally estimated covariances, both estimates converge slower, matching the probabilistic rate of local estimation. (d) *Accurate and precise simulations:* As iterations progress, the proposed algorithm converges faster and yields lower variance of simulated estimates in comparison to the distributed sample-averaging ones in either setting.

This paper is organized as follows: We formulate the distributed MLE mean estimation problem for agents sampling data with private covariances in Section II. Section III presents a PAM to highlight privacy issues in existing algorithms for standard and private versions of DAC for convergent input signals. Section IV introduces the proposed private DAC algorithm in the context of both privately known and estimated information matrices, followed by their privacy and convergence analyses. We present the algorithm to privately estimate average information mean and mean MLE in Section V, and analyze their probabilistic convergence. Section VI empirically evaluates the the privacy and convergence characteristics of the algorithm. Finally, Section VII concludes the paper.

Notation: Define the set of vectors with unit norm as $\mathbb{S}_{d-1} \equiv \{v | v \in \mathbb{R}^d, v^\top v = 1\}$. The operator norm over a matrix $\Sigma \in \mathbb{R}^{d\times d}$ is given as $\|\Sigma\| = \max_{v\in\mathbb{S}_{d-1}} |v^\top \Sigma v|$. The abbreviation w.p. refers to 'with probability'. The 'bar' notation on a random variable (r.v.) x refers to $\bar{x} = x - \mathbb{E}[x]$.

II. Problem Formulation

Assume that the set of n-sensing agents is given by $\mathcal{V} = \{1, \dots, n\}$. Each agent i collects independent and identically distributed (i.i.d.) data $z_{i,t} \in \mathbb{R}^d$ at time step t from an unknown Gaussian density $\mathcal{N}(\mu^\star, (\Omega_i^\star)^{-1})$, with a common finite mean $\mu^\star \in \mathbb{R}^d$ and individual positive definite covariances $\Sigma_i^\star = (\Omega_i^\star)^{-1} \in \mathbb{R}^{d\times d}$. Therefore, the observations satisfy,

Assumption 1. *The observations $z_{i,t}$ are i.i.d. across time t and independent across agents $i \in \mathcal{V}$.*

The agent i aims to estimate a public copy $\hat{\mu}_{i,t}$ of the mean parameter $\mu^\star$, irrespective of whether $\Omega_i^\star$ is privately known or estimated. When the covariance is known, the maximum likelihood estimate of the mean parameter is,

$$\hat{\mu}_{i,t} = \Big(\sum_{i\in\mathcal{V}} \Omega_i^\star\Big)^{-1} \Big(\sum_{i\in\mathcal{V}} \Omega_i^\star \beta_{i,t}\Big), \;\; \beta_{i,t} = \frac{1}{t}\sum_{k=1}^{t} z_{i,k}. \quad (1)$$

When the true information matrix $\Omega_i^\star$ is unknown, the mean MLE estimates $\hat{\mu}_{i,t}$ require an estimate of the matrix. To address this, the agents can use their observations and mean $\beta_{i,t}$ to locally estimate the inverse covariances $\Omega_{i,t}$ as,

$$\Sigma_{i,t} = \frac{1}{t}\sum_{k=1}^{t} (z_{i,k} - \beta_{i,t})(z_{i,k} - \beta_{i,t})^\top, \;\; \Omega_{i,t} = \Sigma_{i,t}^{-1}. \quad (2)$$

To leverage all data and local estimates, the agents communicate over a network characterized by graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. The edge set $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ consists of pairs of agents i, j such that if $(i, j) \in \mathcal{E}$, then the agent j transmits information to agent i. The neighbor set of agent i is given by $\mathcal{V}_i$. Since any connected communication network admits a doubly stochastic representation [33], we assume that the network $\mathcal{G}$ satisfies,

Assumption 2 (Connectivity)**.** *Let $\mathcal{G}$ be an undirected communication network with $|\mathcal{V}| > 2$. The connections are represented by a weighted adjacency matrix A with doubly stochastic weights satisfying $A\mathbf{1}_n = A^\top \mathbf{1}_n = \mathbf{1}_n$, and self-loops denoted by $a_{ii} > 0$. There exists an edge $(i, j) \in \mathcal{E}$ such that the agents i and j are honest.*

At each agent i, the private information matrix signal $\Omega_{i,t}$ converges almost surely to $\Omega_i^\star$. The agents track the dynamic average of information matrix signals via a public variable $\Omega_{i,t}^a$ shared across the network to compute $\frac{1}{n}\sum_{\ell\in\mathcal{V}} \Omega_\ell^\star$. A similar public variable $\nu_{i,t}^a$ tracks the average information mean to enable MLE estimation in (1). To enable secure collaboration over the graph $\mathcal{G}$, we aim to achieve robustness to inference-based privacy attacks from eavesdroppers and internal agents. Please note that the privacy of agents in 2-node network

cannot be protected, because any node can always deduce the information at the neighbor using its average estimates and private inputs.

Apart from all shared messages given by $\Omega^a_{i,t}$, a curious agent can use the doubly stochastic property to infer the matrix A in certain networks. For instance, the central agent in a star network can estimate other weights using the doubly stochasticity constraints over the neighbor weights. Therefore, we assume that any external eavesdroppers have access to the complete matrix A and all shared messages, meaning the information set is $\mathcal{I}_t = \{A, \Omega^a_{i,t} | i \in \mathcal{V}\}$. Although an honest-but-curious internal agent implements the estimation algorithm faithfully, it accesses shared messages, matrix A, and even its internal states to infer others' private variables. Thus, we define a privacy-preserving algorithm as,

Definition 1 (Privacy)**.** *Let each agent i implement distributed algorithm $\mathcal{A}$ to track the average of local signals $\Omega_{i,t}$. If there exist infinitely many variations of local signals $\{\Omega_{i,t} | i \in \mathcal{V}\}$ such that the adversary's information set $\mathcal{I}_t$ consisting of network parameters, shared messages and certain internal states remain unchanged, then the algorithm $\mathcal{A}$ preserves the privacy of local signals.*

Rather than quantifying changes to eavesdroppers' information sets as in differential privacy [16], this definition follows [22] to describe the existence of a set of inputs producing the same information set. This definition admits weaker privacy guarantees in comparison to infinite m-uncertainty notation in [34]. It is chosen to accommodate even positive definite information matrix signals while ensuring the strongest possible privacy guarantee short of the infinite m-uncertainty. Since this privacy definition is stated for arbitrary sequences of $\Omega_{i,t}$, it holds for the noisy variations of input signals. Thus, the resulting privacy-preserving distributed MLE problem is,

Problem 1. *How do the n agents collecting data $\{z_{i,t}\}$ communicate over the graph $\mathcal{G}$ to estimate the MLE $\hat{\mu}_{i,t}$ in (1) at a quantifiable rate of convergence if (a) the true inverse covariance $\Omega^\star_i$ is privately known, or, (b) the private local estimates $\Omega_{i,t}$ probabilistically converge to $\Omega^\star_i$?*

Since MLE depends on the aggregate of privately held information matrices $\Omega^\star_i$, any privacy-preserving estimation method needs to account for convergence of local empirical estimates $\Omega_{i,t}$ in (2). Second-order privacy preserving estimation over probabilistically convergent signals such as $\Omega_{i,t}$ are a characteristic of calibration and localization problems in sensor networks and optimization problem for model learning.

III. Privacy Concerns in Existing Methods

In this section, we describe the static and dynamic average consensus (DAC) algorithms and their SD-based privacy-preserving versions, aiming to track the desired average. For each one, we provide PAMs to extract the original convergent inputs from the publicly accessible information. For the following discussion, let agent i receive a convergent signal $\{\omega_{i,t}\}$ at each time step t. Without loss of generality, this section assumes that the signals $\omega_{i,t} \in \mathbb{R}$ are scalar.

A. Static and Dynamic Average Consensus [31], [35], [36]

In a static consensus algorithm, the agents aim to compute the average of a local fixed value $\omega^\star_i$. For this purpose, the variable $\omega^a_{i,t}$ asymptotically estimates the average $\frac{1}{n}\sum_{i=1}^n \omega^\star_i$ in the distributed algorithm [35] given as $\omega^a_{i,t+1} = \sum_{j=1}^n a_{ij}\omega^a_{j,t}$, $\omega^a_{i,1} = \omega^\star_i$. This algorithm converges [37] at a geometric rate $\mathcal{O}(\lambda^t)$ for some $\lambda \in (0,1)$ dependent on the weights in matrix A. Due to the initialization of shared variables with local values, this algorithm is not private.

If the agents instead receive time-varying signals $\omega_{i,t}$, the DAC algorithm tracks the dynamic average given by $\omega^{av}_t = \frac{1}{n}\sum_{l=1}^n \omega_{l,t}$ via the estimate $\omega^a_{i,t}$ for $t \geq 1$ as,

$$\omega^a_{i,t+1} = \sum_{j=1}^n a_{ij}\omega^a_{j,t} + \Delta\omega_{i,t},\ \Delta\omega_{i,t} = \omega_{i,t+1} - \omega_{i,t}, \quad (3)$$

where we initialize the estimate as $\omega^a_{i,1} = \omega_{i,1}$. The error between the estimate and the dynamic average remains bounded [31], with convergence rate to the bound no worse than $\mathrm{Re}(\lambda_2(A))$, where $\lambda_2(A)$ is the second-largest eigenvalue of matrix A by magnitude. If the input signals converge, the estimates converge to the asymptotic average as a result. Using the shared variables $\omega^a_{i,t}$ and weights a_{ij}, one can track the underlying private signal $\omega_{i,t}$ via the estimator $\hat{\omega}_{i,t}$ using the dynamical update $\hat{\omega}_{i,t+1} = \omega^a_{i,t+1} - \sum_{j=1}^n a_{ij}\omega^a_{j,t} + \hat{\omega}_{i,t}$ with initialization $\hat{\omega}_{i,1} = \omega_{i,1}$. Next, we recall two algorithms relying on the SD approach to preserve signal privacy in static and dynamic averaging consensus algorithms.

B. Private Static Average Consensus

As introduced in [20], the state decomposition approach splits the estimated state at any agent $i \in \mathcal{V}$ into two components, a public accessible $\omega^a_{i,t}$ and a secret privately-held $\omega^s_{i,t}$. With the initialization $\omega^a_{i,0} + \omega^s_{i,0} = 2\omega^\star_i$ and a small $\epsilon > 0$, the agent updates its estimates as follows,

$$\omega^a_{i,t+1} = \epsilon \sum_{j \in \mathcal{V}_i} b_{ij,t}\omega^a_{j,t} + \epsilon \mathbf{b}_{i,t}(\omega^s_{i,t} - \omega^a_{i,t}), \quad (4)$$

$$\omega^s_{i,t+1} = \omega^s_{i,t} + \epsilon \mathbf{b}_{i,t}(\omega^a_{i,t} - \omega^s_{i,t}),\ b_{ii,t} = \frac{1}{\epsilon} - \sum_{j \in \mathcal{V}_i \setminus \{i\}} b_{ij,t},$$

where the weights $b_{ij,0}, \mathbf{b}_{i,0} \in \mathbb{R}$ for $i \neq j$ are selected arbitrarily under the symmetry constraint $b_{ij,0} = b_{ji,0}$. For every $t \geq 1$, the weights lie in the set $(\eta, 1)$ for some $\eta > 0$.

Due to the secret variable, the underlying network in such SD-based algorithms extends the original graph by n additional shadow nodes. Specifically, each shadow node maintains the secret estimate $\omega^s_{i,t}$ and connects solely to the original corresponding agent i. For the combined linear update over states $[(\omega^a_{i,0})^\top, (\omega^s_{i,0})^\top]^\top$, the rows and columns of initial weights sum to one. Despite this, the augmented weight matrix may not be doubly stochastic due to some negative elements.

The estimates are guaranteed to converge as $\lim_{t\to\infty} \omega^a_{i,t} = \frac{1}{n}\sum_{i=1}^n \omega_{i,0}$ while keeping initial values private. But, any trivial extension of this static algorithm alone is insufficient for privately estimating the MLE mean in (1). Even when the agents know their true information matrices privately, the information mean terms $\Omega^\star_i \beta_{i,t}$ remain time-varying.

C. Private Dynamic Average Consensus (PDAC)

For the DAC algorithm, a continuous-time private version has been devised in [22]. Apart from splitting estimates into public and secret versions given by $\omega^a_{i,t}, \omega^s_{i,t}$, corresponding input terms $x^\omega_{i,t}, y^\omega_{i,t}$ are introduced. In contrast to the time varying weights in (4), these components are updated using the fixed weights in A and some $\zeta > 0$. Upon imposing $\zeta \in (0, \min_i a_{ii})$ to enable mixing, we present a discrete time version of the algorithm for any time $t \geq 1$ as,

$$\begin{aligned} \omega^a_{i,t+1} &= \sum_{j=1}^{n} a_{ij}\omega^a_{j,t} + \zeta(\omega^s_{i,t} - \omega^a_{i,t}) + x^\omega_{i,t}, \\ \omega^s_{i,t+1} &= \omega^s_{i,t} + \zeta(\omega^a_{i,t} - \omega^s_{i,t}) + y^\omega_{i,t}, \end{aligned} \tag{5}$$

where the differential signal inputs satisfy $x^\omega_{i,t} + y^\omega_{i,t} = 2\Delta\omega_{i,t} = 2(\omega_{i,t+1} - \omega_{i,t})$, and the public and private estimates are initialized as $\omega^a_{i,1} + \omega^s_{i,1} = 2\omega_{i,1}$. Next, we discuss the challenges in achieving simultaneous privacy and convergence with this algorithm in presence of convergent inputs.

D. Convergence and privacy concerns in PDAC algorithm

The work in [22] establishes that the PDAC estimates are uniformly ultimately bounded [38], implying the existence of a time after which the error between the estimates and the true value remain bounded. While this property ensures that the PDAC algorithm tracks the average signal, it does not guarantee zero estimation error, even if the input signals are convergent. When the agents consider the split satisfying $x^\omega_{i,t} - \zeta_i = y^\omega_{i,t} + \zeta_i = 2\Delta\omega_{i,t}$, critical to preserving privacy in [22], the estimates do not converge to the correct average. We highlight this issue for a 5-agent network in Fig. 1 showing biased estimates for such additive input components, that track the average but do not converge to it.

In this section, we show that a convergent split of the input signal into public and private components $x^\omega_{i,t}, y^\omega_{i,t}$ enforces convergence in the average estimators. For convergent inputs ω_t in consensus algorithms, a convergent split satisfies $\|x^\omega_t\|, \|y^\omega_t\| \leq M\|\Delta\omega_t\|$. But, when the public component $x^\omega_{i,t}$ of the input signal is convergent, privacy is compromised by a PAM capable of tracking the input signal, as devised next. For this PAM, we assume that $\omega^a_t, \omega_t, x^\omega_t$ are vectors of the corresponding signals over the agents at time step t.

Proposition 1. *Assume that the public variables $\{\omega^a_t\}_{t\geq 1}$ and weights A, ζ in the updates (5) are known. Suppose that the public input differences are bounded as $\|x^\omega_t\| \leq g_t$ such that $\lim_{t\to\infty} g_t = 0$. Then, the true signals $\{\omega_t\}_{t\geq 1}$ are estimated at the rate $\mathcal{O}(g_t)$ by the term $\hat{\omega}_t$ in the iterative updates,*

$$\begin{aligned} \hat{\omega}_{t+1} &= \tilde{\omega}_{t+1} + \frac{1}{2\zeta}\tilde{x}^\omega_t, \\ \tilde{x}^\omega_t &= \omega^a_{t+1} - (A - \zeta\mathbb{I})\omega^a_t - \zeta\tilde{\omega}^s_t, \\ \tilde{\omega}^s_t &= \zeta\omega^a_{t-1} + (1-\zeta)\tilde{\omega}^s_{t-1} + (2\Delta\tilde{\omega}_{t-1} - \tilde{x}^\omega_{t-1}), \end{aligned}$$

where $\{\tilde{\omega}_t\}_{t\geq 1}$ is an arbitrary signal sequence, and we initialize $\tilde{\omega}^s_1 = 2\tilde{\omega}_1 - \omega^a_1$ and initialize $\tilde{x}^\omega_1$ arbitrarily.

Proof To construct the eavesdropping attack, we begin by guessing a convergent vectored sequence $\tilde{\omega}_{t+1}$ representing the true signals, and input splits $\tilde{x}^\omega_t, \tilde{y}^\omega_t$ of the corresponding temporal signal differences. The eavesdropper simulates the private dynamic average consensus algorithm with the guessed signals, and the known coefficients A, ζ. A comparison between generated public estimates to the actual ones in ω^a_t yields a functioning PAM. Since the public signals $\{\omega^a_t\}_{t>0}$ remain unchanged for guessed case, the updates in (5) yield,

$$\begin{aligned} &\omega^a_{t+1} = (A - \zeta\mathbb{I})\omega^a_t + \zeta\tilde{\omega}^s_t + \tilde{x}^\omega_t = (A - \zeta\mathbb{I})\omega^a_t + \zeta\omega^s_t + x^\omega_t, \\ &\implies \tilde{x}^\omega_t - x^\omega_t = -\zeta(\tilde{\omega}^s_t - \omega^s_t). \end{aligned} \tag{6}$$

The difference between actual and guessed private variable updates from (5) with substituted inputs $y^\omega_t = 2\Delta\omega_t - x^\omega_t$ is,

$$\tilde{\omega}^s_{t+1} - \omega^s_{t+1} = (1-\zeta)(\tilde{\omega}^s_t - \omega^s_t) + 2(\Delta\tilde{\omega}_t - \Delta\omega_t) - (\tilde{x}^\omega_t - x^\omega_t).$$

Substituting this equation into (6), we obtain the telescoping series on the gap between private estimates in the case of true and guessed signals as,

$$\tilde{\omega}^s_{t+1} - \omega^s_{t+1} = (\tilde{\omega}^s_t - \omega^s_t) + 2(\Delta\tilde{\omega}_t - \Delta\omega_t).$$

Unrolling this over the time steps yields,

$$\begin{aligned} \tilde{\omega}^s_{t+1} - \omega^s_{t+1} &= (\tilde{\omega}^s_0 - \omega^s_0) + 2\sum_{k=0}^{t}(\Delta\tilde{\omega}_k - \Delta\omega_k) \\ &= (\tilde{\omega}^s_0 - \omega^s_0) + 2(\tilde{\omega}_{t+1} - \tilde{\omega}_0 - (\omega_{t+1} - \omega_0)). \end{aligned}$$

Since ω^a_0 remains the same, the true and guessed initial conditions in $\omega^a_0 + \tilde{\omega}^s_0 = 2\tilde{\omega}_0$ and $\omega^a_0 + \omega^s_0 = 2\omega_0$ imply that $\tilde{\omega}^s_0 - \omega^s_0 = 2(\tilde{\omega}_0 - \omega_0)$. Therefore, we have,

$$2(\tilde{\omega}_{t+1} - \omega_{t+1}) = \tilde{\omega}^s_{t+1} - \omega^s_{t+1} = -(1/\zeta)(\tilde{x}^\omega_t - x^\omega_t). \tag{7}$$

Since the input component x^ω_t in (7) converges at the rate $\mathcal{O}(g_t)$, we construct an estimator $\hat{\omega}_{t+1}$ with matching convergence rate, in terms of the guessed signals and public inputs,

$$\hat{\omega}_{t+1} = \tilde{\omega}_{t+1} + \frac{1}{2\zeta}\tilde{x}^\omega_t, \ \|\hat{\omega}_{t+1} - \omega_{t+1}\| = \frac{1}{2\zeta}\|x^\omega_t\|.$$

The update rules on $\tilde{x}^\omega_t$ and $\tilde{\omega}^s_t$ follow from public and private variable updates in (5). ■

For simulating the privacy preserving estimator in (5), we compute the PDAC-based average of time-varying signals shown in Fig. 1 (left) for a network of $n = 5$ agents. We first show estimates generated for additive splitting of inputs, as required for privacy in the proof of [22]. These estimates in red track the variations signal average but remain biased in comparison to standard DAC algorithm.

To remove this bias for accurate estimation, we run PDAC algorithm with convergent public input splits $x^\omega_{i,t}$ at the agents. In this setting, the eavesdropper recovers the original signals $\omega_{i,t}$ at each agent by implementing the PAM in Prop. 1 using its access to the public average estimates $\omega^a_{i,t}$ and weights A, ζ. Fig. 1 (right) plots the eavesdropper's estimate $\hat{\omega}_{i,t}$ over the original signals.

This discussion does not contradict the bounded error guarantees in [22], but boundedness does not yield accurate MLE mean estimates while agent covariances are kept private. Therefore, the next section will extend this algorithm to

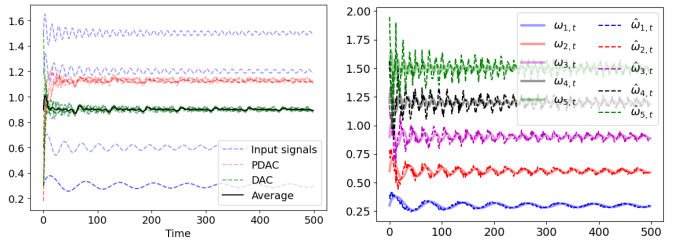

Fig. 1. PDAC cannot simultaneously achieve accurate tracking and privacy. In an $n = 5$ agent network, agent i privately observes $\omega_{i,t} = 0.3i + \frac{0.03}{\sqrt{t}}\sin(0.1it)$. (Left) Biased tracking: public estimates $\omega^a_{i,t}$ in PDAC algorithm (5) (red dashed) deviate from the true average $\bar{\omega}_t = \frac{1}{n}\sum_{i=1}^n \omega_{i,t}$ (black solid). The estimates are computed using privacy-preserving splits $x^\omega_{i,t} = 2\alpha_t\Delta\omega_{i,t} + \xi$, $y^\omega_{i,t} = 2\Delta\omega_{i,t} - x_{i,t}$ for $\xi = 0.2$, $\alpha_t \in (0,1)$. (Right) Input recovery: When public components of input signal differences decay asymptotically, i.e. $\|x^\omega_{i,t}\| \to 0$, an eavesdropper uses Prop. 1 to generate estimates $\hat{\omega}_{i,t}$ (dashed) that reconstruct private signals $\omega_{i,t}$ (solid).

address the simultaneous privacy and accurate convergence issues in estimating the true average of information matrices.

IV. Privacy-preserving consensus algorithms

In this section, we propose a privacy-preserving distributed algorithm for estimating averages, tailored to averaging the local information matrices at agents. We begin by introducing the proposed algorithms and discussing their implementation, followed by privacy and convergence guarantees. Combining the resulting matrix average estimates with corresponding information mean terms yields the MLE mean in (1). An extension of these algorithms to information mean averages in the following section thus completes the proposed algorithm.

First, we discuss the local running estimates of local mean and information matrix. When the true information matrix $\Omega^\star_i$ is unknown, the agents use their observations to estimate it recursively at iteration t as,

$$\Omega_{i,t} = \Sigma^{-1}_{i,t},\ \Sigma_{i,t} = \alpha_{i,t} - \beta_{i,t}\beta^\top_{i,t}, \tag{8}$$
$$\beta_{i,t} = \frac{t-1}{t}\beta_{i,t-1} + \frac{1}{t}z_{i,t},\ \alpha_{i,t} = \frac{t-1}{t}\alpha_{i,t-1} + \frac{1}{t}z_{i,t}z^\top_{i,t},$$

where the terms $\alpha_{i,t}$ and $\beta_{i,t}$ correspond to the averages of squared and linear terms of the observations at the agent i. These local estimates act as the input signals to the algorithm prescribed to estimate the mean MLE privately.

This section presents a private dynamic consensus algorithm to estimate the average of the true local information matrices. While presented for positive definite matrices, the algorithm holds for arbitrary time-varying tall matrices and vectors. When these matrices are known, the algorithm needs to keep them private. In case of local estimates converging to the information matrices in (8), the algorithm ought to preserve the privacy of the entire sequence given by $\{\Omega_{i,t} | t \geq 1\}$.

A. Convergent Private DAC for Information Matrices

To address the tracking of convergent inputs in the algorithm via the PAM proposed in Subsection III-C, we extend the state decomposition approach by introducing an initial mixing step and signal difference induced bounds on the public and private input splits. Let each agent $i \in \mathcal{V}$ maintain two estimates of the average input Ω^{av}_t at time t, given by publicly shared $\Omega^a_{i,t} \in \mathbb{R}^{d\times d}$, and a privately held $\Omega^s_{i,t} \in \mathbb{R}^{d\times d}$. The mixing step at the beginning of the proposed algorithm is,

$$\begin{aligned}\Omega^a_{i,1} &= \sum_{j\in\mathcal{V}_i} B_{ij}\Omega^a_{j,0} + \mathcal{B}_i(\Omega^s_{i,0} - \Omega^a_{i,0}),\\ \Omega^s_{i,1} &= \Omega^s_{i,0} + \mathcal{B}_i(\Omega^a_{i,0} - \Omega^s_{i,0}),\end{aligned} \tag{9}$$

where the public and private estimates are initialized as,

$$\Omega^a_{i,0} + \Omega^s_{i,0} = 2\Omega_{i,1}, \quad \forall i \in \mathcal{V}. \tag{10}$$

The inter-agent block matrices $B_{i\ell} \in \mathbb{R}^{d\times d}$ constrain the sum $\sum_{i\in\mathcal{V}_\ell} B_{i\ell} = \mathbb{I}_d$ at each column $\ell \in \mathcal{V}$ and satisfy $B_{i\ell} = 0$ if $(i,\ell) \notin \mathcal{E}$. This column sum constraint preserves the aggregated estimates as $\sum_{i=1}^n(\Omega^a_{i,1} + \Omega^s_{i,1}) = 2\sum_{i=1}^n \Omega_{i,1}$. The coupling matrix $\mathcal{B}_i \in \mathbb{R}^{d\times d}$ is chosen locally. For $\zeta \in (0, \min_i a_{ii})$, any future updates are,

$$\begin{aligned}\Omega^a_{i,t+1} &= \sum_{j=1}^n a_{ij}\Omega^a_{j,t} + \zeta(\Omega^s_{i,t} - \Omega^a_{i,t}) + X^\Omega_{i,t},\\ \Omega^s_{i,t+1} &= \Omega^s_{i,t} + \zeta(\Omega^a_{i,t} - \Omega^s_{i,t}) + Y^\Omega_{i,t},\end{aligned} \tag{11}$$

with input signal components defined in terms of differential signal inputs $\Delta\Omega_{i,t} = \Omega_{i,t+1} - \Omega_{i,t}$ and $M > 1$ as,

$$X^\Omega_{i,t} + Y^\Omega_{i,t} = 2\Delta\Omega_{i,t},\ \|X^\Omega_{i,t}\|, \|Y^\Omega_{i,t}\| \leq M\|\Delta\Omega_{i,t}\|. \tag{12}$$

In the known setting, the information matrix $\Omega_{i,t} = \Omega^\star_i$ implying that $\Delta\Omega_{i,t} = X^\Omega_{i,t} = Y^\Omega_{i,t} = 0$. When estimated locally, agents compute $\Omega_{i,t}$ recursively using (8).

Here, the individual agents estimate an accessible copy $\Omega^a_{i,t}$ tracking the running average $\Omega^{av}_t = \frac{1}{n}\sum_{l=1}^n \Omega_{l,t}$ of input signals. As we quantify later, the input constraints are introduced to enable convergent behavior in the presence of convergent signals of the form $\Omega_{i,t}$. The initial mixing step is key to avoiding loss of privacy. After discussing some insights, the following subsections establish the privacy and convergence characteristics of this algorithm.

Remark 1. The block column sum condition on the components B_{ij} of matrix $B \in \mathbb{R}^{nd\times nd}$ subsumes block column stochasticity, as the individual components may not remain positive. Agent i chooses the coupling matrix $\mathcal{B}_i$ arbitrarily.

Remark 2. This algorithm merges the initialization based on the average-preserving principle in SD-based static algorithm [20] with time-varying input splitting in continuous-time dynamic version [22], and introduces additional input constraints to facilitate simultaneous privacy and accurate convergence. This presentation generalizes the implementation for both the static and dynamic averaging settings. For the static setting where $\Delta\Omega_{i,t} = 0$, this algorithm reduces to the proposal in [20]. We show that the additional input constraints are crucial for convergence in the dynamic setting with convergent inputs.

Remark 3. The communication load due to the shared variables in this privacy preserving version at each iteration remains the same as the standard consensus algorithm.

Remark 4. The coupling weight $\mathcal{B}_i$ can be selected arbitrarily and stored locally at each agent $i \in \mathcal{V}$, avoiding any informa-

tion leakage. The requirement on number of agents $|\mathcal{V}| > 2$ in Assumption 2 avoids trivially revealing the weights via $B_{jj} = \mathbb{I}_d - B_{ij}$. Due to the column sum constraint on the inter-agent weights B_{ij}, we propose a distributed scheme based on homomorphic encryption with Paillier's cyptosystem in Appendix C to generate them in a privacy preserving manner.

Remark 5. The requirements on initializing estimates in (10) and input components in (12) can be satisfied locally at each agent. The arbitrarily chosen initial estimate $\Omega^a_{i,0}$ can even be negative. For input components, select an arbitrary but uniformly bounded matrix $\Xi_{i,t} \in \mathbb{R}^{d\times d}$ at time t such that $\|\Xi_{i,t}\| \leq M$ and subsequently define the components as $X_{i,t} = \Xi_{i,t}\Delta\Omega_{i,t}, Y_{i,t} = (2\mathbb{I} - \Xi_{i,t})\Delta\Omega_{i,t}$ at each time t.

B. Privacy Analysis

To preserve privacy, the algorithm ought to be able to yield the same public information even if the private information such as true information matrix has been modified. We will show this form of privacy in both the static and dynamic settings, where the information sets available to the eavesdropper and an internal curious agent ℓ are,

$$\begin{aligned}\mathcal{I}_t &= \left\{A, \Omega^a_{r,k} | r \in \mathcal{V}, k \leq t\right\},\\ \mathcal{I}_{\ell,t} &= \mathcal{I}_t \cup \left\{B_{\ell r}, \mathcal{B}_\ell, \Omega^s_{\ell,k} | r \in \mathcal{V}, k \leq t\right\}.\end{aligned} \tag{13}$$

For any neighbors $(i,j) \in \mathcal{E}$, we show that the application of proposed algorithm to any perturbation of signals $\Omega_{i,t}, \Omega_{j,t}$ that preserve the signal average Ω^{av}_t may also preserve the information available to an eavesdropper or curious agents.

Proposition 2. *For neighbors $i,j \in \mathcal{E}$ with $i \neq j$, consider the mixing step (9) with perturbed inputs $\tilde{\Omega}_{i,1}, \tilde{\Omega}_{j,1}$ that satisfy $\tilde{\Omega}_{i,1}+\tilde{\Omega}_{j,1} = \Omega_{i,1}+\Omega_{j,1}$. Then, there exist modified inter-agent and coupling weights $\{\tilde{B}_{r\ell}, \tilde{\mathcal{B}}_\ell | r, \ell \in \{i,j\}\}$, with all other weights unchanged, and satisfying the column sum constraints $\sum_{r\in\mathcal{V}_\ell} \tilde{B}_{r\ell} = \mathbb{I}$ for all $\ell \in \mathcal{V}$ such that the public and private estimates at times $t \in \{0,1\}$ satisfy*

$$\tilde{\Omega}^a_{\ell,0} = \Omega^a_{\ell,0}, \quad \tilde{\Omega}^a_{\ell,1} = \Omega^a_{\ell,1}, \quad \tilde{\Omega}^s_{\ell,1} = \Omega^s_{\ell,1}, \quad \forall \ell \in \mathcal{V}.$$

Proof Consider a distinct execution of the mixing step in (9) with modified inputs $\tilde{\Omega}_{\ell,t}$, inter-agent and coupling weights $\tilde{B}_{r\ell}, \tilde{\mathcal{B}}_\ell$ and public and private estimates $\tilde{\Omega}^a_{\ell,t}, \tilde{\Omega}^s_{\ell,t}$, where these quantities differ from the original only for the neighbors $\ell \in \{i,j\}$. When the inputs preserve the average via $\tilde{\Omega}_{i,1}+\tilde{\Omega}_{j,1} = \Omega_{i,1}+\Omega_{j,1}$, we construct the set of admissible weights $\tilde{B}_{r\ell}, \tilde{\mathcal{B}}_\ell$ for $r, \ell \in \{i,j\}$ that preserve the public and private estimates $\{\tilde{\Omega}^a_{\ell,t}, \tilde{\Omega}^s_{\ell,t}\}$ for all agents $\ell \in \mathcal{V}$ at $t = 1$.

Using the initialization condition $\tilde{\Omega}^a_{\ell,0} + \tilde{\Omega}^s_{\ell,0} = 2\tilde{\Omega}_{\ell,1}$ similar to (10), but with modified inputs at the neighbors $\ell \in \{i,j\}$, we select private estimates $\tilde{\Omega}^s_{\ell,0}$ to preserve the public estimates at $t = 0$ as,

$$\tilde{\Omega}^a_{\ell,0} = \Omega^a_{\ell,0}; \; \tilde{\Omega}^s_{\ell,0} = \Omega^s_{\ell,0} + 2(\tilde{\Omega}_{\ell,1} - \Omega_{\ell,1}), \forall \ell \in \{i,j\}. \tag{14}$$

The estimates $\tilde{\Omega}_{\ell,1}, \tilde{\Omega}^a_{\ell,0}, \tilde{\Omega}^s_{\ell,0}$ at other agents $\ell \in \mathcal{V}\backslash\{i,j\}$ are conserved. Now, we show the existence of admissible weights $\tilde{B}_{ij}, \tilde{\mathcal{B}}_i$ that preserve the agent estimates for any admissible $\tilde{\Omega}_{i,1}$. Preserving the secret variable as $\tilde{\Omega}^s_{i,1} = \Omega^s_{i,1}$ via (9),

$$\tilde{\mathcal{B}}_i(\tilde{\Omega}^a_{i,0} - \tilde{\Omega}^s_{i,0}) = (\Omega^s_{i,0} - \tilde{\Omega}^s_{i,0}) + \mathcal{B}_i(\Omega^a_{i,0} - \Omega^s_{i,0}), \tag{15}$$

simplified with (14) and initialization in (10) yields $\tilde{\mathcal{B}}_i$ as,

$$\tilde{\mathcal{B}}_i = ((\Omega_{i,1} - \tilde{\Omega}_{i,1}) + \mathcal{B}_i(\Omega^a_{i,0} - \Omega_{i,1}))(\Omega^a_{i,0} - \tilde{\Omega}_{i,1})^{-1}.$$

At agent j, we similarly have $\tilde{\mathcal{B}}_j = (\Omega_{j,1} - \tilde{\Omega}_{j,1} + \mathcal{B}_j(\Omega^a_{j,0} - \Omega_{j,1}))(\Omega^a_{j,0} - \tilde{\Omega}_{j,1})^{-1}$. Next, we consider preserved public variables, with $\tilde{\Omega}^a_{i,1} = \Omega^a_{i,1}$ and $\tilde{\Omega}^a_{j,1} = \Omega^a_{j,1}$. Since $\tilde{B}_{i\ell} = B_{i\ell}$ for any $\ell \neq i,j$ and $\tilde{\Omega}^a_{\ell,0} = \Omega^a_{\ell,0}$ in $\Omega^a_{i,1} = \sum_{\ell=1}^n B_{i\ell}\Omega^a_{\ell,0} + \mathcal{B}_i(\Omega^s_{i,0} - \Omega^a_{i,0})$, setting $\tilde{\Omega}^a_{i,1} = \Omega^a_{i,1}$ in (9) yields,

$$\begin{aligned}&\tilde{B}_{ii}\Omega^a_{i,0} + \tilde{B}_{ij}\Omega^a_{j,0}\\ &= B_{ii}\Omega^a_{i,0} + B_{ij}\Omega^a_{j,0} + \mathcal{B}_i(\Omega^s_{i,0} - \Omega^a_{i,0}) - \tilde{\mathcal{B}}_i(\tilde{\Omega}^s_{i,0} - \Omega^a_{i,0})\\ &= B_{ii}\Omega^a_{i,0} + B_{ij}\Omega^a_{j,0} + (\Omega^s_{i,0} - \tilde{\Omega}^s_{i,0}) \qquad \text{(Using (15))}\\ &= B_{ii}\Omega^a_{i,0} + B_{ij}\Omega^a_{j,0} + 2(\Omega_{i,1} - \tilde{\Omega}_{i,1}) \qquad (16)\end{aligned}$$

Similarly, upon setting $\tilde{\Omega}^a_{j,1} = \Omega^a_{j,1}$,

$$\tilde{B}_{ji}\Omega^a_{i,0} + \tilde{B}_{jj}\Omega^a_{j,0} = B_{ji}\Omega^a_{i,0} + B_{jj}\Omega^a_{j,0} + 2(\Omega_{j,1} - \tilde{\Omega}_{j,1}). \tag{17}$$

In addition, we have the column sum constraints given as,

$$\tilde{B}_{ii} + \tilde{B}_{ji} = B_{ii} + B_{ji}, \tag{18a}$$

$$\tilde{B}_{ij} + \tilde{B}_{jj} = B_{ij} + B_{jj}. \tag{18b}$$

Using the average preserving nature of input signals and positive definiteness of estimates $\Omega^a_{i,0}, \Omega^a_{j,0}$, we can show that (16) is a linear combination of the other three equations as (18a)$*\Omega^a_{i,0}$+ (18b)$*\Omega^a_{j,0}$ - (17). Given four unknowns and only three independent linear equations, there exist infinitely many solutions to the matrices $\tilde{B}_{ii}, \tilde{B}_{ij}, \tilde{B}_{ji}, \tilde{B}_{jj}$.

Thus, for any modification $\tilde{\Omega}_{i,1} < \Omega_{i,1}+\Omega_{j,1}$, one can pick an initial input $\tilde{\Omega}_{j,1}$, inter-agent weights $\tilde{B}_{ii}, \tilde{B}_{ij}, \tilde{B}_{ji}, \tilde{B}_{jj}$, and coupling weights $\tilde{\mathcal{B}}_i, \tilde{\mathcal{B}}_j$ such that the agents' public and private estimates remain unchanged at time step 1. Moreover, by (18a), the weights at $t = 0$ still preserve column sums. ■

In this proof, we see that the required weight modifications are limited to weight matrices of any two arbitrary neighbors (i,j), consisting of $\tilde{B}_{ii}, \tilde{B}_{ij}, \tilde{B}_{ji}, \tilde{B}_{jj}, \tilde{\mathcal{B}}_i, \tilde{\mathcal{B}}_j$. This allows preserving privacy in presence of internal agents as well.

Theorem 1. *For the static input version of the algorithm in (9)-(11) over an undirected network, an eavesdropper with information set $\mathcal{I}_t$ or any internal agent ℓ with information set $\mathcal{I}_{\ell,t}$ in (13) cannot infer the true information matrix $\Omega^\star_i$ if agent i has an honest neighbor $j \neq \ell$.*

Proof As a result of Prop. 2, there exist admissible modifications to weights $B_{ii}, B_{ij}, B_{ji}, B_{jj}, \mathcal{B}_i, \mathcal{B}_j$ at neighbors (i,j) that preserve all estimates at time step 1 under any average preserving changes to signals $\Omega_{i,1}, \Omega_{j,1}$. In the static setting, we set $\Omega_{i,t} = \Omega^\star_i$ implying that the term $\Delta\Omega_{i,t} = 0$ and subsequently inputs $X^\Omega_{i,t}, Y^\Omega_{i,t} = 0$ for all time steps. Therefore, the estimates at time step 1 determine all subsequent estimates. Since these estimates can be invariant for any average-preserving modification to neighboring signals, the privacy of true information matrices

is preserved under the proposed algorithm. In the case of an internal agent ℓ, the privacy is preserved for any modifications to a pair of connected agents (i,j) because the additional items in the information set $\mathcal{I}_{\ell,t}$ do not further constrain the modifications to the weights stipulated via (15)-(18b) in the proof to Prop. 2. ■

In the dynamic setting, the local estimate $\Omega_{i,t}$ is incorporated in the estimate while maintaining its privacy. Therefore, we show the existence of admissible signal difference bounded sequence of public and private inputs $X_{i,t}, Y_{i,t}$, that produce the same public information set for a range of variations to the estimated information matrices at all time steps.

Theorem 2. *For the algorithm in (9)-(11), an eavesdropper with information set $\mathcal{I}_t$ or curious agent $\mathcal{I}_{\ell,t}$ in (13) cannot accurately estimate the private covariance sequence $\Omega_{i,t} \to \Omega_i^\star$ if agent i has an honest neighbor $j \neq \ell$.*

Proof As in the static case, we consider an average preserving modification to the inputs of honest neighbors (i,j) distinct from the curious agent ℓ given by $\tilde{\Omega}_{i,t}, \tilde{\Omega}_{j,t}$ for all $t \geq 1$ constructed as follows,

$$\tilde{\Omega}_{i,t} = \Omega_{i,t} + P^\star, \tilde{\Omega}_{j,t} = \Omega_{j,t} - P^\star, P^\star \in \mathbb{R}^{d\times d}. \tag{19}$$

This construction preserves signal average via $\tilde{\Omega}_{i,t} + \tilde{\Omega}_{j,t} = \Omega_{i,t} + \Omega_{j,t}$, with level of privacy quantified as $\rho = \|P^\star\|$. When the signals are real-valued, the privacy level ρ can be arbitrarily large by selecting $P^\star$ with large norm. When the signals $\Omega_{i,t}, \Omega_{j,t}$ are positive-definite instead, the privacy level ρ is limited by the smallest eigenvalue of these information matrices, as $P^\star \preceq \Omega_{i,t}, \Omega_{j,t}, \forall t \geq 1$ to ensure that the modified signals remain positive-definite. A general version of this proof exists for time-varying privacy levels ρ_t by allowing $P^\star$ to be time-varying as well, but we focus on the constant privacy level for simplicity. This proof establishes that any such input sequence may yield the same set of public variables.

At agent i, we define the modified input splits as $\{\tilde{X}^\Omega_{i,t}, \tilde{Y}^\Omega_{i,t}\}$, and the corresponding estimates as $\{\tilde{\Omega}^a_{i,t}, \tilde{\Omega}^s_{i,t}\}$. From Prop. 2, there exist admissible initial weights that preserve the public and private estimates at time step 1 as,

$$\tilde{\Omega}^a_{\ell,1} = \Omega^a_{\ell,1},\ \tilde{\Omega}^s_{\ell,1} = \Omega^s_{\ell,1},\ \forall \ell \in \mathcal{V}. \tag{20}$$

After this time step, the algorithm runs with fixed weights A, ζ. We prove via induction on iteration indices that the following estimates with preserved public variables are observed at each agent for certain admissible splits $\{\tilde{X}^\Omega_{i,t}, \tilde{Y}^\Omega_{i,t}\}$,

$$\tilde{\Omega}^a_{\ell,t} = \Omega^a_{\ell,t}, \tilde{\Omega}^s_{\ell,t} = \Omega^s_{\ell,t}, \forall \ell \in \mathcal{V}. \tag{21}$$

For the base case, the following signal inputs preserve the public variable value $\tilde{\Omega}^a_{i,2} = \Omega^a_{i,2}$ at $t = 2$,

$$\begin{aligned} &\tilde{X}^\Omega_{i,1} = X^\Omega_{i,1}, \tilde{Y}^\Omega_{i,1} = 2\Delta\tilde{\Omega}_{i,1} - \tilde{X}^\Omega_{i,1}, \\ &\Delta\tilde{\Omega}_{i,1} = \tilde{\Omega}_{i,2} - \tilde{\Omega}_{i,1} = \Omega_{i,2} - \Omega_{i,1} = \Delta\Omega_{i,1}, \end{aligned} \tag{22}$$

where the last equality follows from our construction in (19). With the requirement on input components in (12),

$$\tilde{Y}^\Omega_{i,1} - Y^\Omega_{i,1} = 2\Delta\tilde{\Omega}_{i,1} - Y^\Omega_{i,1} - X^\Omega_{i,1} = 2(\Delta\tilde{\Omega}_{i,1} - \Delta\Omega_{i,1}) = 0. \tag{23}$$

Using the preserved estimates at $t = 1$ in (20), the private variable $\tilde{\Omega}^s_{i,2}$ is expressed using (11) in terms of unchanged input component $\tilde{Y}^\Omega_{i,1}$ from (23) to yield

$$\tilde{\Omega}^s_{i,2} - \Omega^s_{i,2} = \tilde{Y}^\Omega_{i,1} - Y^\Omega_{i,1} = 0.$$

Now, assuming that the hypothesis on agent estimates in (21) holds until time step t, the public estimate at time $t+1$ satisfies $\tilde{\Omega}^a_{i,t+1} = \Omega^a_{i,t+1}$ for the following inputs,

$$\tilde{X}^\Omega_{i,t} = X^\Omega_{i,t}, \quad \tilde{Y}^\Omega_{i,t} = Y^\Omega_{i,t}, \tag{24}$$

As a result, we have $\tilde{\Omega}^s_{i,t+1} = \Omega^s_{i,t+1}$, resulting from the induction hypothesis in (21). Following similar steps for agent j at time step $t+1$, one can prove that the private and public estimates remain unchanged as $\tilde{\Omega}^s_{\ell,t+1} = \Omega^s_{\ell,t+1}, \forall \ell \in \mathcal{V}$, and $\tilde{\Omega}^a_{\ell,t+1} = \Omega^a_{\ell,t+1}, \forall \ell \in \mathcal{V}$.

Finally, we verify that the altered inputs $\tilde{X}^\Omega_{\ell,t}, \tilde{Y}^\Omega_{\ell,t}$ for $\ell \in \{i,j\}$ remain bounded as defined in (12). This follows trivially from (24) which establishes that

$$\Delta\tilde{\Omega}_{i,t} = \frac{1}{2}(\tilde{X}^\Omega_{i,t} + \tilde{Y}^\Omega_{i,t}) = \frac{1}{2}(X^\Omega_{i,t} + Y^\Omega_{i,t} = \Delta\Omega_{i,t}),$$

implying that $\|\tilde{X}^\Omega_{i,t}\| = \|X^\Omega_{i,t}\| \leq M\|\Delta\Omega_{i,t}\| = M\|\Delta\tilde{\Omega}_{i,t}\|$ and $\|\tilde{Y}^\Omega_{i,t}\| \leq M\|\Delta\tilde{\Omega}_{i,t}\|$ similarly.

Therefore, an adversary cannot distinguish between a sequence $\Omega_{i,t}$ converging to $\Omega_i^\star$ and another sequence $\tilde{\Omega}_{i,t}$ with any admissible gap $P^\star$ between them. ■

This proof shows that the same public and private signal splits can be used for any biased but average-preserving version of the original signal sequences to generate the same public estimates at all agents. For real-valued signals, the privacy guarantees in this section hold for any arbitrary deviations from $\Omega_{i,t}, \Omega_{j,t}$, matching infinite m-uncertainty privacy in [34]. Although, when the signals and its alternatives are required to be positive definite, the privacy level may be quantified by $\min(\lambda_{\min}(\Omega_{i,t}), \lambda_{\min}(\Omega_{j,t}))$, where $\lambda_{\min}(\cdot)$ is the smallest eigenvalue of the positive definite matrices in the argument. This ensures that the modified signals remain positive-definite. When the original information matrices are small, the resulting privacy level is small as well, reflecting the fact that the associated large covariances are relatively uninformative. Having established the nature of privacy granted by this algorithm, we now analyze its convergence behavior.

C. Convergence Analysis

We analyze the convergence rates of the agent estimates to the network-wide average of true information matrices, whether it is known or estimated locally. First, we express the algorithm as a linear system, then present intermediate technical results needed to subsequently establish deterministic and probabilitic convergence rates in the known and unknown covariance settings respectively.

At $t = 0$, the arbitrariness and sum preserving nature of the weights B_{ij} leads to maintaining privacy and allowing convergence respectively. But the rate of convergence depends on the weights in A, ζ defining the updates at subsequent time steps. Upon defining vectorized estimates and inputs as $\Omega_t^a = [(\Omega_{1,t}^a)^\top \cdots (\Omega_{n,t}^a)^\top]^\top$ and correspondingly Ω_t^s, X_t, Y_t and $A_c^\otimes = A_c \otimes \mathbb{I}_d$, this algorithm updates linearly at any time step $t \geq 1$ as,

$$\begin{bmatrix}\Omega_{t+1}^a \\ \Omega_{t+1}^s\end{bmatrix} = A_c^\otimes \begin{bmatrix}\Omega_t^a \\ \Omega_t^s\end{bmatrix} + \begin{bmatrix}X_t \\ Y_t\end{bmatrix}, A_c = \begin{bmatrix}A - \zeta\mathbb{I} & \zeta\mathbb{I} \\ \zeta\mathbb{I} & (1-\zeta)\mathbb{I}\end{bmatrix}. \quad (25)$$

The doubly stochastic matrix A_c corresponds to a connected graph with loops to a shadow version of each node. Since the update to the public parameter $\Omega_{i,t+1}^a$ depends on the matrix A_c^t, we compute its second eigenvalue to characterize the rate of its convergence to $\frac{1}{2n}\mathbf{1}_{2n}\mathbf{1}_{2n}^\top$ as follows,

Lemma 1. *For any $\zeta \in (0, \min_i \{a_{ii} | \forall i \in \mathcal{V}\})$, the matrix A_c in (25) is doubly stochastic and its second eigenvalue $\lambda_2(A_c) \in (0,1)$ satisfies,*

$$\lambda_2(A_c) = \max\left\{\lambda_c^+(\max_i\{\lambda_i | \lambda_i \neq 1\}), -\lambda_c^-(\min_i\{\lambda_i\})\right\},$$

where λ_i are the eigenvalues of doubly stochastic matrix A and $\lambda_c^\pm(\lambda) = \frac{(1+\lambda) \pm \sqrt{(1-\lambda)^2 + 4\zeta^2}}{2} - \zeta$. In addition, the magnitude of the second-largest eigenvalue $|\lambda_2(A_c)|$ of matrix A_c is greater than the corresponding eigenvalue $|\lambda_2|$ of matrix A.

Proof Please refer to Appendix A. ■

Since the second eigenvalue determines the rate of mixing, the consensus estimates converge slower in the private setting due to the connectivity over $2n$ variables. This can be attributed to the structure of matrix A_c, representing a graph containing n shadow nodes connected only to their counterparts in graph $\mathcal{G}$.

Let us represent element (i,j) in the matrix raised to the power $t-k$ as $[A^{t-k}]_{ij} = 1/n + \gamma_{ij}^{t,k}$ with bounds on $\gamma_{ij}^{t,k}$ as,

Lemma 2. *From [39], the error $|[A_c^{t-k}]_{ij} - 1/2n| \leq \lambda^{t-k}$ for an undirected static network is given as,*

$$\lambda = \min\left\{(1 - 1/(4(2n)^3)), \sqrt{\lambda_2(A_c)}\right\} \in (0,1),$$

where $\lambda_2(A_c)$ is the second-largest eigenvalue of matrix A_c.

Averaging known covariance: Based on Lemma 2, we can now compute a deterministic convergence rate of the estimates to the average information matrices $\frac{1}{n}\sum_{i\in\mathcal{V}}\Omega_i^\star$ for known local covariances.

Proposition 3. *When the local covariances are known, the information matrix $\Omega_{i,t}^a$ in (11) converges to the average of true information matrices as $\|\Omega_{i,t}^a - \Omega_{av}^\star\|_F \leq c\lambda^t$ for the positive constant $c = 4n^2\|\Omega_{av}^\star\|_F$ with $\Omega_{av}^\star = \frac{1}{n}\sum_{i\in\mathcal{V}}\Omega_i^\star$.*

Proof Since the matrix B is sum-preserving, the sum of estimates is preserved across the initial step as,

$$\begin{aligned}\sum_{i=1}^n(\Omega_{i,1}^a + \Omega_{i,1}^s) &= \sum_{i=1}^n\sum_{j=1}^n B_{ij}\Omega_{j,0}^a + \sum_{i=1}^n \Omega_{i,0}^s \\ &= \sum_{j=1}^n\Big(\sum_{i=1}^n B_{ij}\Big)\Omega_{j,0}^a + \sum_{i=1}^n\Omega_{i,0}^s = \sum_{i=1}^n(\Omega_{i,0}^a + \Omega_{i,0}^s).\end{aligned} \quad (26)$$

Substituting the initialization condition $\Omega_{i,0}^a + \Omega_{i,0}^s = 2\Omega_i^\star$, we note that the average of true information matrices satisfies,

$$\Omega_{av}^\star = \frac{1}{n}\sum_{i\in\mathcal{V}}\Omega_i^\star = \frac{1}{2n}\sum_{i=1}^n(\Omega_{i,1}^a + \Omega_{i,1}^s). \quad (27)$$

Using the (i,j)th element of matrix A_c^t, the public estimates $\Omega_{i,t}^a$ for the static version of update (11) at time t relate to initial values as,

$$\begin{aligned}\Omega_{i,t+1}^a &= \sum_{j=1}^n [A_c^t]_{ij}\Omega_{j,1}^a + \sum_{j=n+1}^{2n}[A_c^t]_{ij}\Omega_{j-n,1}^s, \\ \Omega_{i,t+1}^s &= \sum_{j=1}^n [A_c^t]_{i+n,j}\Omega_{j,1}^a + \sum_{j=n+1}^{2n}[A_c^t]_{i+n,j}\Omega_{j-n,1}^s.\end{aligned} \quad (28)$$

From Lemma 2, the elements of doubly stochastic matrix A_c can be expressed as $[A_c^t]_{ij} = \frac{1}{2n} + \gamma_{ij}^{t,0}$ where $\|\gamma_{ij}^{t,0}\| \leq \lambda^t$. Substituting this expression in (28) to bound the gap between estimates and the average $\Omega_{av}^\star$,

$$\begin{aligned}\|\Omega_{i,t+1}^a - \Omega_{av}^\star\|_F = \Bigg\| &\frac{1}{2n}\Big(\sum_{j=1}^n\Omega_{j,1}^a + \sum_{j=n+1}^{2n}\Omega_{j-n,1}^s\Big) \\ &+ \sum_{j=1}^n\gamma_{ij}^{t,0}\Omega_{j,1}^a + \sum_{j=n+1}^{2n}\gamma_{ij}^{t,0}\Omega_{j-n,1}^s - \Omega_{av}^\star\Bigg\|_F.\end{aligned}$$

Using the initialization relation in (27), the estimation error is bounded as follows,

$$\|\Omega_{i,t+1}^a - \Omega_{av}^\star\|_F \leq \lambda^t\Big\|\sum_{j=1}^n\Omega_{j,1}^a + \sum_{j=1}^n\Omega_{j,1}^s\Big\| = 4n^2\|\Omega_{av}^\star\|_F\lambda^t.$$

■

Due to the linear updates after the initial mixing in (9), the estimates converge to the true average $\Omega_{av}^\star$ at a geometric rate determined by the second eigenvalue of matrix A_c.

Estimated local information matrix: Now, we can study the dynamic version of (11) where the local covariances are estimated by first looking at the convergence rate of the input covariance estimates, which drives the convergence of its inverse, namely the information matrices.

Lemma 3 ([40, Theorem 5.7])**.** *For any $\delta \in (0,1)$, the empirical covariance matrix $\Sigma_{i,t}$ in (2) computed with i.i.d. samples from $\mathcal{N}(\mu^\star, \Sigma_i^\star)$ satisfies the probabilistic bound:*

$$\mathbb{P}\left(\left\|\Sigma_{i,t} - \Sigma_i^\star\right\|_{\text{op}} \leq \left\|\Sigma_i^\star\right\|_{\text{op}}\sqrt{\frac{d + \log(1/\delta)}{t}}\right) \geq 1 - \delta,$$

given in terms of the operator norm $\|\Sigma\|_{\text{op}} = \sqrt{\lambda_{\max}(\Sigma^\top\Sigma)}$.

Based on the convergence of the empirical covariances in Lemma 3, we examine the convergence of the information

matrix estimates to the average $\Omega^\star_{av} = \frac{1}{n}\sum_{i\in\mathcal{V}}\Omega^\star_i$. For this purpose, we will present an intermediate algebraic result to determine the rate of convergence of the estimates.

Lemma 4. *The sum $S_t = \sum_{k=1}^t \frac{\lambda^{t-k}}{k^\alpha}$, with $\alpha > 0$ and $\lambda \in (0,1)$ is bounded above for any sufficiently large $t > t_0 = \lceil \frac{\lambda^{1/\alpha}}{1-\lambda^{1/\alpha}} \rceil$ as $S_t < ct^{-\alpha}$ for some $c > 0$.*

Proof Please see Appendix A for a general derivation with $S_t = \sum_{k=1}^t \frac{\lambda^{t-k}}{k^\alpha}$ for $\alpha > 0$. ■

We use this lemma to compute a deterministic geometric convergence rate of the agent estimates to $\Omega^\star_{av}$.

Lemma 5. *For a sufficiently large t_0 and w.p. at least $(1-\delta)$, the public estimates in (9)-(11) at any agent $i \in \mathcal{V}$ is bounded above at any $t > t_0$ for $\Omega^\star_{av} = \frac{1}{n}\sum_{l=1}^n \Omega^\star_l$ some $c > 0$ as,*

$$\|\Omega^a_{i,t+1} - \Omega^\star_{av}\|_F \leq \frac{c}{\sqrt{t+1}}.$$

Proof At $t = 0$, the sum of variables is preserved as $\sum_{i=1}^n \Omega^a_{i,1} + \Omega^s_{i,1} = \sum_{i=1}^n \Omega^a_{i,0} + \Omega^s_{i,0}$. Define the public error matrix $E_{i,t} = \Omega^a_{i,t} - \Omega^{av}_t$ and its private counterpart $E^s_{i,t} = \Omega^s_{i,t} - \Omega^{av}_t$ with the average signal $\Omega^{av}_t = \frac{1}{n}\sum_{l=1}^n \Omega_{l,t}$. The gap to estimated average is dynamically updated in terms of information matrices as,

$$\begin{aligned} E_{i,t+1} &= \sum_{j=1}^n A_{c,ij}E_{j,t} + \sum_{j=n+1}^{2n} A_{c,ij}E^s_{j-n,t} + X^\Omega_{i,t} - \Delta\Omega^{av}_t \\ &= \sum_{j=1}^n [A^t_c]_{ij}E_{j,1} + \sum_{j=n+1}^{2n} [A^t_c]_{ij}E^s_{j-n,1} \qquad (29) \\ &+ \sum_{k=1}^t \Big\{ \sum_{j=1}^n [A^{t-k}_c]_{ij}X^\Omega_{j,k} + \sum_{j=n+1}^{2n} [A^{t-k}_c]_{ij}Y^\Omega_{j-n,k} - \Delta\Omega^{av}_k \Big\}. \end{aligned}$$

Since the initializations satisfy $\frac{1}{n}\sum_{i=1}^n(\Omega^a_{i,1} + \Omega^s_{i,1}) = 2\Omega^{av}_1$, the initial error matrix average in (29) satisfies,

$$\begin{aligned} &\Big\| \sum_{j=1}^n [A^t_c]_{ij}E_{j,1} + \sum_{j=n+1}^{2n} [A^t_c]_{ij}E^s_{j-n,1} \Big\| \\ &= \Big\| \sum_{j=1}^n [A^t_c]_{ij}(\Omega^a_{j,1} - \Omega^{av}_1) + \sum_{j=n+1}^{2n} [A^t_c]_{ij}(\Omega^s_{j-n,1} - \Omega^{av}_1) \Big\| \\ &= \Big\| \sum_{j=1}^n \Big([A^t_c]_{ij} - \frac{1}{2n}\Big)\Omega^a_{j,1} + \sum_{j=n+1}^{2n} \Big([A^t_c]_{ij} - \frac{1}{2n}\Big)\Omega^s_{j-n,1} \Big\| \\ &\leq \lambda^t \sum_{j=1}^n (\|\Omega^a_{j,1}\| + \|\Omega^s_{j,1}\|), \end{aligned}$$

where the final step with λ in Lemma 2 depends on the second largest eigenvalue λ_2 of matrix A_c computed in Lemma 1.

Next, we focus on the temporal terms in (29) by substituting $[A^{t-k}_c]_{ij} = \gamma^{c,t-k}_{ij} + 1/2n$ and then simplifying with $\sum_{j=1}^n (X^\Omega_{j,k} + Y^\Omega_{j,k}) = 2\Delta\Omega^{av}_k$. This yields the upper bound,

$$\begin{aligned} \|E_{i,t+1}\|_F &\leq \lambda^t \sum_{j=1}^n (\|\Omega^a_{j,1}\| + \|\Omega^s_{j,1}\|) \qquad (30) \\ &+ \Big\| \sum_{k=1}^t \Big\{ \sum_{j=1}^n \gamma^{c,t-k}_{ij} X^\Omega_{j,k} + \sum_{j=n+1}^{2n} \gamma^{c,t-k}_{ij} Y^\Omega_{j-n,k} \Big\} \Big\|. \end{aligned}$$

Due to the algorithm requirement bounding the individual signal components in terms of total signal difference $\Delta\Omega_t$,

$$\begin{aligned} \|E_{i,t+1}\|_F &\leq \lambda^t \sum_{j=1}^n (\|\Omega^a_{j,1}\| + \|\Omega^s_{j,1}\|) \\ &+ M \sum_{k=1}^t \Big\{ \sum_{j=1}^n (\|\gamma^{c,t-k}_{ij}\| + \|\gamma^{c,t-k}_{i,j+n}\|)\|\Delta\Omega_{j,k}\| \Big\}. \qquad (31) \end{aligned}$$

From the bound in Lemma 2, the convergence of communication matrix satisfies $|\gamma^{c,t-k}_{ij}| \leq \lambda^{t-k}$. Since $\|\Delta\Omega_{j,k}\| \leq \|\Omega_{j,k+1} - \Omega^\star_j\| + \|\Omega^\star_j - \Omega_{j,k}\|$, we use the probabilistic bound of $1/\sqrt{k}$ on local information matrix differences in Lemma S2 to imply that $\|\Delta\Omega_{j,k}\| \leq c_2/\sqrt{k}$. Due to the logical implication, the following holds w.p. $(1-\delta)$ as well,

$$\|E_{i,t+1}\|_F \leq c_1\lambda^t + 2c_2 \sum_{k=1}^t \frac{\lambda^{t-k}}{\sqrt{k}},$$

Now, we simplify with the temporal average estimate Ω^{av}_{t+1} to upper bound the gap to the true average $\Omega^\star_{av}$ as,

$$\begin{aligned} \|\Omega^a_{i,t+1} - \Omega^\star_{av}\|_F &\leq \|E_{i,t+1}\|_F + \frac{1}{n}\sum_{l=1}^n \|\Omega_{l,t+1} - \Omega^\star_l\|_F \\ &\leq c_1\lambda^t + 2c_2 \sum_{k=1}^t \frac{\lambda^{t-k}}{\sqrt{k}} + \frac{c}{\sqrt{t+1}}. \end{aligned}$$

From Lemma 4, the probabilistic upper bound is given by $c/\sqrt{t+1}$ for some constant $c > 0$ and sufficiently large t. ■

Remark 6. While this probabilistic bound is given for $\mathcal{O}(1/\sqrt{t+1})$ due to the convergence rate of the local signals, the guarantee can be provided for any algorithm converging at a rate of $\mathcal{O}(t^{-\alpha})$ for any $\alpha > 0$.

In this section, we presented a privacy-preserving DAC algorithm for convergent signals such as information matrices. When the information matrix is privately known, a deterministic geometric convergence rate to the true average is established. When it is estimated statistically, the estimates follow the local convergence rate. Now, we will extend these results to information mean and then compute the MLE mean.

V. Privacy Preserving Mean MLE Estimation

In this section, we extend the algorithm proposed for information matrices in (9) - (12) to information mean terms, in order to estimate the MLE mean in (1) while keeping the true information matrices and observations private. Each agent tracks average information mean with a public and private estimate given as $\nu^a_{i,t}, \nu^s_{i,t}$. Analogous to (9), agents select arbitrary coupling and inter-agent weight matrices $\mathcal{B}^\nu_i, B^\nu_{ij} \in \mathbb{R}^{d\times d}$

subject to the column sum constraint $\sum_{i=1}^n B_{ij}^\nu = \mathbb{I}_d$ and network connections as $B_{ij}^\nu = 0$ if $(i,j) \notin \mathcal{E}$. The initial mixing step then follows as,

$$\begin{aligned}\nu_{i,1}^a &= \sum_{j=1}^n B_{ij}^\nu \nu_{j,0}^a + \mathcal{B}_i^\nu(\nu_{i,0}^s - \nu_{i,0}^a),\\ \nu_{i,1}^s &= \nu_{i,0}^s + \mathcal{B}_i^\nu(\nu_{i,0}^a - \nu_{i,0}^s).\end{aligned} \tag{32}$$

The estimates are initialized as $\nu_{i,0}^a + \nu_{i,0}^s = 2\Omega_{i,1}\beta_{i,1}$. At subsequent time steps $t \geq 1$, the updates resemble (11) as,

$$\begin{aligned}\nu_{i,t+1}^a &= \sum_{j=1}^n a_{ij}\nu_{j,t}^a + \zeta(\nu_{i,t}^s - \nu_{i,t}^a) + x_{i,t}^\nu,\\ \nu_{i,t+1}^s &= \nu_{i,t}^s + \zeta(\nu_{i,t}^a - \nu_{i,t}^s) + y_{i,t}^\nu,\end{aligned} \tag{33}$$

with the differential signal inputs satisfying for some $M > 0$,

$$\begin{aligned}&x_{i,t}^\nu + y_{i,t}^\nu = 2(\Omega_{i,t+1}\beta_{i,t+1} - \Omega_{i,t}\beta_{i,t}),\\ &\|x_{i,t}^\nu\|, \|y_{i,t}^\nu\| \leq M\|\Omega_{i,t+1}\beta_{i,t+1} - \Omega_{i,t}\beta_{i,t}\|,\end{aligned}$$

computed locally via (8), with $\Omega_{i,t} = \Omega_i^\star$ in case of known true covariances. The mean is thus privately estimated as,

$$\mu_{i,t+1} = (\Omega_{i,t+1}^a)^{-1}\nu_{i,t+1}^a, \tag{34}$$

where the average information matrix $\Omega_{i,t+1}^a$ was estimated for known and unknown covariance cases in (9)-(11). In the subsequent analysis, the term $\nu_{i,t}$ corresponds to $\Omega_i^\star\beta_{i,t}$ in the case of known true covariance and $\Omega_{i,t}\beta_{i,t}$ in the case of unknown covariance. The distributed estimate $\mu_{i,t}$ in (34) aims to track the MLE mean $\hat{\mu}_{i,t}$ in (1) for finite t, and we will show that both converge to $\mu^\star$ at rate $\mathcal{O}\left(1/\sqrt{nt}\right)$ in the case of known covariances.

A. Privacy Analysis

Since the term $\nu_{i,t}$ is time-varying in case of both known and unknown true covariances, we prove the algorithm's privacy in presence of dynamic inputs. This analysis follows the privacy proof to averaging of information matrices in Prop. 2 and Thm. 2.

Proposition 4. *There exist admissible modifications to inter-agent and coupling weights $B_{ii}^\nu, B_{ij}^\nu, B_{ji}^\nu, B_{jj}^\nu, \mathcal{B}_i^\nu, \mathcal{B}_j^\nu$ such that all public and private estimates at time step 1 are preserved for the initial mixing step in (9) under any average-preserving perturbation to the input signals $\nu_{i,1}, \nu_{j,1}$.*

Proof This derivation is a trivial adaptation of the proof to Prop. 2 for a vector setting, yielding more admissible modifications to the matrix weights compared to the possibilities in case of information matrices. ■

Even for the known covariance setting, the signal $\nu_{i,t} = \Omega_i^\star\beta_{i,t}$ is time-varying. Therefore, we study the privacy preservation of the algorithm for a convergent input next.

Theorem 3. *For the algorithm in (32)-(33), an eavesdropper with information set $\mathcal{I}_t^d = \{A, \nu_{i,t}^a | \forall i \in \mathcal{V}\}$ cannot accurately estimate the private information mean $\nu_{i,t} \to \Omega_i^\star\mu^\star$ at any agent in an undirected network. In addition, any honest-but-curious node ℓ cannot estimate the information mean $\nu_{i,t}$ if agent i has a neighbor $j \neq \ell$.*

Proof This derivation follows from a trivial adaptation of the proof to Thm. 2 for vectors instead of matrices. ■

Next, we analyze the convergence of average information mean in static and dynamic local covariance inputs, and extend it to the mean MLE estimates.

B. Convergence analysis with known covariance

For the static setting with known covariance, we express the next technical lemma to establish consensus based improvements to the rate of convergence of average information mean estimates, which are then extended to MLE mean terms.

Lemma 6. *The normalized local sample given by $\bar{\beta}_{i,k} = \beta_{i,k} - \theta^\star$ at agent i and time k satisfy,*

$$\mathbb{E}[\bar{\beta}_{i,k_1}^\top \bar{\beta}_{j,k_2}] = \begin{cases}(\operatorname{tr}(\Sigma_i^\star)/\max\{k_1,k_2\}) & \text{if } i = j,\\ 0 & \text{otherwise.}\end{cases}$$

Therefore, the expected product of local mean differences is,

$$\mathbb{E}[(\bar{\beta}_{i,k_1+1} - \bar{\beta}_{i,k_1})^\top(\bar{\beta}_{j,k_2+1} - \bar{\beta}_{j,k_2})] = \begin{cases}0 & \text{if } k_1 \neq k_2,\\ 0 & \text{if } i \neq j,\\ \frac{\operatorname{tr}(\Sigma_i^\star)}{k_1(k_1+1)} & \text{otherwise,}\end{cases}$$

where $\Sigma_i^\star$ are true covariance matrices.

Proof The first statement follows from the independence in Assumption 1. When $k_1 > k_2$, $\max\{k_1, k_2+1\} = k_1$. The expectation $\mathbb{E}[(\bar{\beta}_{i,k_1+1} - \bar{\beta}_{i,k_1})^\top(\bar{\beta}_{i,k_2+1} - \bar{\beta}_{i,k_2})]$ thus equals,

$$\left(k_1^{-1} + (k_1+1)^{-1} - k_1^{-1} - (k_1+1)^{-1}\right)\operatorname{tr}(\Sigma_i^\star) = 0.$$

The result similarly holds for $k_2 > k_1$. ■

This result allows us to compute a near centralized rate of convergence for estimation in known covariance setting.

Theorem 4. *For the algorithm in (33) with known true covariances, the estimates $\bar{\nu}_{i,t} = \nu_{i,t}^a - \nu^\star$ satisfy,*

$$\mathbb{E}[\|\bar{\nu}_{i,t+1}\|_2^2] \leq \frac{\frac{1}{n}\sum_{j=1}^n c_j}{n(t+1)} + c_{22}\lambda_c^{2t} + \frac{c_{33}}{t^2} + \frac{c_{12}\lambda_c^t}{n(t+1)} + c_{23}\frac{\lambda_c^t}{t^2},$$

for $c_j = \operatorname{tr}(\Omega_j^\star)$ and constants $c_{22}, c_{33}, c_{12}, c_{23} > 0$ with similar bounds on expected value of $\nu_{i,t}^s$.

Proof Please see Appendix B. ■

This expected upper bound informs a probabilistic upper bound for the information mean estimates for sufficiently large time steps by dropping faster decaying terms.

Corollary 1. *For the algorithm in (33) with known true covariances, the estimates $\nu_{i,t}^a, \nu_{i,t}^s$ converge probabilistically to the optimal value $\nu^\star$ at a rate of $\mathcal{O}(1/\sqrt{nt})$ after sufficiently large time step $t_0 > 0$.*

Proof We express the probabilistic bound on the information mean estimate and use Markov's inequality on the squared terms to obtain $\mathbb{P}(\|\nu_{r,t} - \nu^\star\|_2 \geq \epsilon) \leq \frac{1}{\epsilon^2}\mathbb{E}[\|\bar{\nu}_{r,t}\|_2^2]$. Since $\lambda_c \in (0,1)$, we can use Thm. 4 to drop faster decaying terms with $\frac{1}{t^2}$ and λ_c^t for sufficiently large time steps t to obtain

$\mathbb{P}(\|\nu_{r,t} - \nu^\star\|_2 \geq \epsilon) \leq \mathcal{O}\left(\frac{\frac{1}{n}\sum_{j=1}^n c_j}{nt}\right)$. ■

While Lemma 1 implies that the magnitude of the second-largest eigenvalue increases in tandem with ζ, this eigenvalue impacts only the transient convergence rate terms of the proposed algorithm derived in Corollary 1. We now use this result in conjunction with convergence of information matrix estimates in case of known true covariance to upper bound the convergence rate of private MLE mean estimate in (34).

Theorem 5. *When the covariance is known, the error $\|\mu_{i,t} - \mu^\star\|_F$ is probabilistically bounded above for sufficiently large time steps t and some $c > 0$ as,*

$$\left\|\mu_{i,t} - \left(\frac{1}{n}\sum_{l=1}^n \Omega_l^\star\right)^{-1}\left(\frac{1}{n}\sum_{l=1}^n \nu_l^\star\right)\right\|_F \leq \frac{c}{\sqrt{nt}}.$$

Proof As per Prop. 3, the public variable $\Omega_{i,t}^a$ converges to $\frac{1}{n}\sum_{l=1}^n \Omega_l^\star$ at the rate of $c\lambda^t$ for sufficiently large t. With Lemma S1, its inverse $(\Omega_{i,t}^a)^{-1}$ converges at the same rate as the matrix after sufficiently large t. Similarly, per Corollary 1, the public variable $\nu_{i,t}^a$ probabilistically converges to $\frac{1}{n}\sum_{l=1}^n \nu_l^\star$ at the rate of $c/\sqrt{nt}$. Thus, their product in $\mu_{i,t} = (\Omega_{i,t}^a)^{-1}\nu_{i,t}^a$ converges at the same rate to the true MLE mean given as $(\frac{1}{n}\sum_{l=1}^n \Omega_l^\star)^{-1}\frac{1}{n}\sum_{l=1}^n \nu_l^\star = (\frac{1}{n}\sum_{l=1}^n \Omega_l^\star)^{-1}(\frac{1}{n}\sum_{l=1}^n \Omega_l^\star\mu^\star) = \mu^\star$. ■

C. Convergence analysis with unknown covariance

This subsection analyzes the case where the sensors estimate their $\Omega_{i,t}$ online, showing that the convergence rate of the estimate $\mu_{i,t}$ is determined by the local estimates.

Lemma 7. *For the algorithm in (33) with unknown covariances, the information mean estimate $\nu_{i,t}^a$ converges probabilistically as $\|\nu_{i,t}^a - \frac{1}{n}\sum_{l=1}^n \nu_l^\star\|_F \leq c/\sqrt{t}$.*

Proof The proof follows the steps in Lemma 5 using the convergence rate for information mean differences $\|\nu_{i,t+1} - \nu_{i,t}\|$ in Lemma S3. ■

Theorem 6. *In case of unknown local covariances, the private MLE mean estimate $\mu_{i,t}$ in (34) converges probabilistically to $\mu^\star$, satisfying the following bound for sufficiently large time steps t and some constant $c > 0$ as,*

$$\left\|\mu_{i,t} - \left(\frac{1}{n}\sum_{l=1}^n \Omega_l^\star\right)^{-1}\left(\frac{1}{n}\sum_{l=1}^n \nu_l^\star\right)\right\|_F \leq \frac{c}{\sqrt{t}}.$$

Proof As per Lemma 5, the public variable $\Omega_{i,t}^a$ converges to $\frac{1}{n}\sum_{l=1}^n \Omega_l^\star$ at the rate of $c/\sqrt{t}$ for sufficiently large t. Similarly, per Lemma 7, the public variable $\nu_{i,t}^a$ converges to $\frac{1}{n}\sum_{l=1}^n \nu_l^\star$ at the rate of $c/\sqrt{t}$. Further, the matrix inverse $(\Omega_{i,t}^a)^{-1}$ converges at the same rate, thus its product with $\nu_{i,t+1}^a$ converges at the same rate to $\mu^\star$. ■

Remark 7. The state-decomposition algorithms such as [22] introduce additional virtual nodes that increases the second eigenvalue λ_c (see Lemma 1). But, the convergence rate of second order estimates such as $\Omega_{i,t}^a$ depends jointly on the mixing and the local signals, with the local signals determining the order of convergence in both known mean (Thm. 4) and unknown mean (Thm. 6) settings.

VI. Simulation

This work deals with the privacy-preserving cooperative estimation problem, where agents aim to estimate a common parameter that is dependent on their private data and noise characteristics. In particular, we consider a network of $n = 5$ sensing agents, with agent $i \in \mathcal{V}$ collecting i.i.d. Gaussian samples $z_{i,t} \sim \mathcal{N}(\mu^\star, \Sigma_i^\star)$ with common but unknown mean $\mu^\star$ and covariance $\Sigma_i^\star$. The data and covariance are held privately at each agent, and the covariance is either known or locally estimated at the run time. While preserving privacy of the data sequence $\{z_{i,t}\}$ and the sensing capability encoded via covariance $\Sigma_i^\star$, the agents collaborate over a connected network to estimate the true mean $\mu^\star$ with minimal variance.

This section compares the convergence of MLE mean estimated via proposed algorithms to those based on DAC, and local and consensus sample averages. To clarify the benefits of MLE, we first describe a distributed sample averaging method with the same order of convergence as the centralized average. In simulation, we compare its convergence to proposed MLE estimates, and use the PAM in Prop. 1 to verify that the exchanged estimates do not leak the true information matrices. Over repeated runs with same data generating distributions, we compare the time evolution of the estimates' error and variance for the proposed algorithms.

A. Distributed sample averaging

Considering the collaboration in the network, a consensus based sample average to estimate the unknown mean μ is,

$$\mu_{i,t} = \frac{1}{t}\Big((t-1)\sum_{j\in\mathcal{V}_i} a_{ij}\mu_{j,t-1} + z_{i,t}\Big). \tag{35}$$

This agent estimate is a weighted average over all prior observations given as $\mu_{i,t} = \frac{1}{t}(\sum_{k=1}^t \sum_{j=1}^n [A^{t-k}]_{ij} z_{j,k})$. Since the matrix product A^k remains row stochastic for any $k > 0$, the expected value of the estimator is $\mathbb{E}[\mu_{i,t}] = \mu^\star$.

Lemma 8. *Let any agent $i \in \mathcal{V}$ estimate the true mean $\mu^\star$ as $\mu_{i,t}$ at iteration t using (35). The probability that estimation error $\|\mu_{i,t} - \mu^\star\|_2$ exceeds $\epsilon > 0$ is bounded as $\mathbb{P}(\|\mu_{i,t} - \mu^\star\|_2 \geq \epsilon) \leq \frac{c}{tn\epsilon^2}$, for some $c > 0$ and number of agents n.*

Following the approach in the proof to Thm. 4, it can be verified that the estimates in (35) indeed converge at the rate of $\mathcal{O}(1/\sqrt{nt})$. The estimate accuracy improves with increasing number of agents n and the amount of sampled data t, with their product matching the convergence in the centralized setting. This result implies that with probability at least $1-\delta$, the estimate $\|\mu_{i,t} - \mu^\star\|_2$ at agent i is bounded by $\sqrt{\frac{c}{tn\delta}}$.

B. Comparing convergence across sample traces

First, we show that the distributed MLE of the mean term in (1) exhibits lower variance for heterogenous data variances.

We consider a five agent connected line network with agents sampling Gaussian densities with individual covariances $\Sigma_i^\star$ to estimate a common mean $\mu^\star = [-1, 1]^\top$. Fig. 2 plots the mean and variance of 50-traces of the estimates $\mu_{i,t}$ generated by the sample averaging in (35) and the proposed algorithm in Sec. V, under both known and unknown covariance settings. The weight matrices $B, \mathcal{B}$ are selected arbitrarily under the column sum constraint, matrix A is doubly stochastic and $0 < \zeta < \min_i a_{ii}$. Fig. 2(a) shows that when the agents sample data with equal covariance, the estimate traces have a similar variance for the three algorithms. In contrast, Fig. 2(b) shows that the estimates resulting from proposed algorithms in (34) exhibit lower variance than sample averages in case of distinct covariances $\Sigma_i^\star = i^{-3}\mathbb{I}_2$, as the distinct covariances accentuate the need for MLE due to disparate measurement quality.

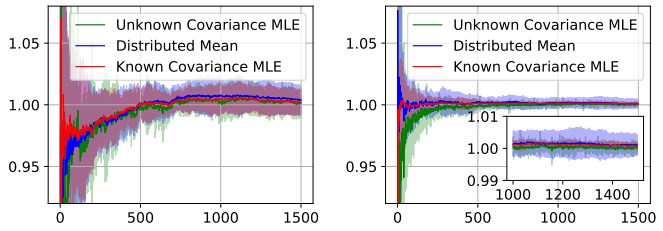

Fig. 2. Plotting mean and variance for the second element estimates in $\mu^\star = [-1, 1]$ over 50 traces of the distributed average and proposed algorithm for known and unknown covariances in homogenous $\Sigma_i^\star = \mathbb{I}_2$ (left) and heterogeneous $\Sigma_i^\star = i^{-3}\mathbb{I}_2$ (right) cases for a 5 agent line network.

While the distributed sample mean and known covariance MLE converge rapidly with the rate of convergence known to match centralized setting, the unknown covariance MLE traces exhibit lower variance only after sufficient iterations. To observe this phenomena, Fig. 3 plots logarithmic error traces of the proposed algorithms, along with the local and sample average estimates. We compute the errors in these four algorithms across 50 data traces, while preserving the network matrix terms A, ζ and initial weight matrices $B, \mathcal{B}$.

The convergence rates of sample average and known covariance proposal match centralized setting given by $\mathcal{O}(1/\sqrt{nt})$, as established in Corollary 1 and Lemma 8 respectively. As per Thm. 6, the mean estimates in case of unknown covariance should converge at the rate of $\mathcal{O}(t^{-1/2})$ for sufficient large $t > 0$, similar to that of the local estimates $\beta_{i,t}$ in (1). In contrast, the simulated estimates perform similar to the known covariance setting after initial iterations. This is due to the superior convergence characteristics of MLE over sample averages as the local covariance estimates get accurate enough.

Fig. 3 reveals that both proposed algorithms eventually outperform sample averaging and local mean. The low variance of estimates in unknown covariance case happens when the local sample covariance is of sufficient quality after a certain number of iterations, roughly 2000 in this instance. Thus, the accuracy of the local information matrices after the early iterations impacts the performance of proposed algorithms.

Next, we compare estimates of standard DAC algorithm in (3) to the proposed known covariance MLE. Fig. 4(a) shows

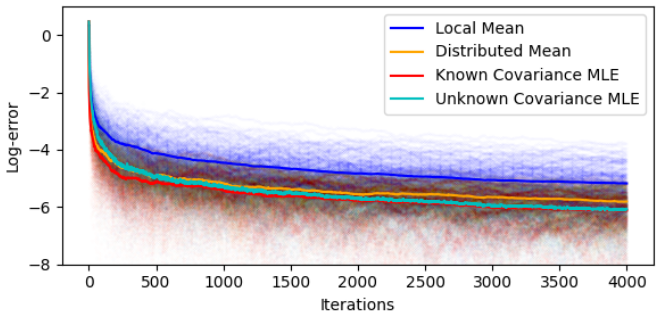

Fig. 3. Plotting the logarithmic error in estimates for $\mu^\star = [-1, 1]$ over 50 traces of the local, distributed consensus and proposed algorithm in known and unknown covariance settings with $\Sigma_i^\star = i^{-2}\mathbb{I}_2$.

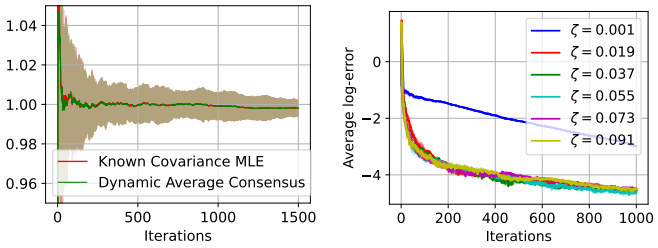

Fig. 4. Comparing mean and variance (left) for the second element estimates in $\mu^\star = [-1, 1]$ between DAC and proposed algorithm and the logarithmic error (right) for multiple ζ values over 50 traces of the proposed algorithm in known covariance settings with $\Sigma_i^\star = i^{-2}\mathbb{I}_2$.

that both estimates exhibit similar variance, implying that SD-based privacy measures have minimal impact on convergence for this network. Fig. 4(b) investigates the convergence rate of proposed algorithm with increasing ζ by plotting the mean of logarithmic errors for a single agent over 50 traces. In the limit where $\zeta = 0$, there is no mixing between public and private variables with $\lambda_c = 1$ per Lemma 1. The term λ_c has monotonic relationship with ζ. For sufficiently small $\zeta = 0.001$ in Fig. 4(b), the early convergence is determined by λ_c^{2t} instead of $\frac{1}{n(t+1)}$ as seen in the upper bound terms of Thm. 4. Therefore, a sufficiently large ζ should be selected to enable fast convergence.

C. Recovering private signals

We consider a 5 sensor network tracking the average of locally estimated information matrices using PDAC in (5) and unknown covariance case of proposed algorithm in (11). The proposed algorithm and PDAC are implemented with input constraints in (12) to allow accurate convergence for both. The locally estimated information matrix inputs $\Omega_{i,t}$ are plotted as translucent precision terms in Fig. 5. The network contains one incredibly precise sensor named Agent 1, whose identity needs to be kept private.

To find sensor precision, an external eavesdropper accesses all shared variables such as $\{\omega_{i,t}^a\}$ in PDAC and $\{\Omega_{i,t}^a\}$ in the proposed algorithm. It has the knowledge of the network structure and inter-agent weights a_{ij} as well. The eavesdropping PAM designed in Prop. 1 is used to recover signals $\hat{\Omega}_{i,t}$ that are plotted as dashed lines in Fig. 5. We observe that

the local information matrix estimates converge to zero error under PDAC, but not for the proposed algorithm.

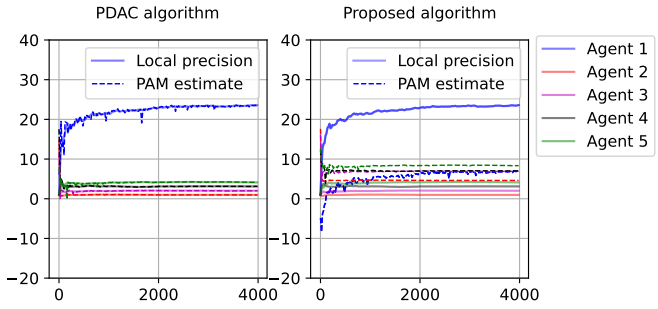

Fig. 5. Recovered private information matrix inputs from public estimates in PDAC and proposed algorithm in a five agent line network.

VII. Conclusion

This paper designs a privacy-preserving distributed MLE estimation algorithm that handles known and estimated local covariances by augmenting dynamic averaging for time varying signals with state decomposition mechanism. To ensure privacy, an initialization step must mix up the decomposed states by distributing generating the mixing matrices. Masking and homomorphic methods can be leverages to generate the matrices, and for completeness, the supplementary material outlines a homomorphic encryption scheme to generate initial mixing matrices that preserve network-wide estimate aggregates without exposing individual signals. Future studies may explore more efficient alternatives to private and distributed generation of such weights. The SD approach avoids repeated encryption costs beyond the generation of mixing weights while communicating same amount of information as a standard distributed algorithm. While adequate for tracking, we show that the existing private SD algorithm is vulnerable to eavesdroppers when estimating convergent signals. Then, we propose modifications to maintain data and covariance privacy while estimating the MLE mean irrespective of the agents' knowledge of their true covariances. Our analysis establishes probabilistic convergence rates, matching the centralized rate with known covariances and the local rate with estimated covariances. In simulations, the proposed algorithms perform similar to their non-private variants, and outperform local and consensus sample averages after initial iterations.

This proposed algorithm for convergent estimates applies to distributed estimation and inference problems dealing with decaying signals. For instance, it lets agents perform consensus over gradients to converge to a common solution in distributed optimization problems, where the knowledge of gradients may expose the agent objectives. The convergence analysis in this work can be improved by finding a tighter bound for the unknown covariance setting.

References

[1] S. Addanki, K. Garbe, E. Jaffe, R. Ostrovsky, and A. Polychroniadou, "Prio+: Privacy preserving aggregate statistics via boolean shares," in *Int. Conf. Secur. Cryptog. Netw.*, pp. 516–539, Springer, 2022.

[2] A. Smith, "Privacy-preserving statistical estimation with optimal convergence rates," in *Proc. Annu. ACM Symp. Theory Comput.*, pp. 813–822, 2011.

[3] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, "Minimax optimal procedures for locally private estimation," *J. Am. Stat. Assoc.*, vol. 113, no. 521, pp. 182–201, 2018.

[4] B. Charrow, N. Michael, and V. Kumar, "Cooperative multi-robot estimation and control for radio source localization," *Int. J. Robot. Res.*, vol. 33, no. 4, pp. 569–580, 2014.

[5] P. Paritosh, N. Atanasov, and S. Martinez, "Distributed Bayesian estimation of continuous variables over time-varying directed networks," *IEEE Control Syst. Lett.*, vol. 6, pp. 2545–2550, 2022.

[6] L. Huang, J. Wu, D. Shi, S. Dey, and L. Shi, "Differential privacy in distributed optimization with gradient tracking," *IEEE Trans. Autom. Control*, vol. 69, no. 9, pp. 5727–5742, 2024.

[7] P. Paritosh, N. Atanasov, and S. Martínez, "Distributed bayesian estimation in sensor networks: Consensus on marginal densities," *IEEE Trans. on Netw. Sci. Eng.*, vol. 12, no. 4, pp. 2848–2862, 2025.

[8] M. H. DeGroot, "Reaching a consensus," *J. Am. Stat. Assoc.*, vol. 69, no. 345, pp. 118–121, 1974.

[9] A. Olshevsky and J. N. Tsitsiklis, "Convergence Speed in Distributed Consensus and Averaging," *SIAM J. Control. Optim.*, vol. 48, pp. 33–55, Jan. 2009.

[10] A. Jadbabaie, P. Molavi, A. Sandroni, and A. Tahbaz-Salehi, "Non-Bayesian social learning," *Games Econ. Behav.*, vol. 76, pp. 210–225, Sept. 2012.

[11] M. Kossek and M. Stefanovic, "Survey of recent results in privacy-preserving mechanisms for multi-agent systems," *J. Intell. Robot. Syst.*, vol. 110, no. 3, p. 129, 2024.

[12] C. N. Hadjicostis and A. D. Domínguez-García, "Privacy-preserving distributed averaging via homomorphically encrypted ratio consensus," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3887–3894, 2020.

[13] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?," in *Proc. 3rd ACM Workshop Cloud Comput. Secur.*, pp. 113–124, 2011.

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

[15] Y. Lu, Z. Yu, and N. Suri, "Privacy-preserving decentralized federated learning over time-varying communication graph," *ACM Trans. Priv. Secur.*, vol. 26, no. 3, pp. 1–39, 2023.

[16] J. He, L. Cai, and X. Guan, "Differential private noise adding mechanism and its application on consensus algorithm," *IEEE Trans. on Signal Process.*, vol. 68, pp. 4069–4082, 2020.

[17] W. Zhang, Z. Zuo, Y. Wang, and G. Hu, "How much noise suffices for privacy of multiagent systems?," *IEEE Trans. on Autom. Control*, vol. 68, no. 10, pp. 6051–6066, 2022.

[18] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private average consensus with optimal noise selection," *IFAC-PapersOnLine*, vol. 48, no. 22, pp. 203–208, 2015.

[19] 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, 2016.

[20] Y. Wang, "Privacy-preserving average consensus via state decomposition," *IEEE Trans. Autom. Control*, vol. 64, no. 11, pp. 4711–4716, 2019.

[21] X. Chen, L. Huang, L. He, S. Dey, and L. Shi, "A differentially private method for distributed optimization in directed networks via state decomposition," *IEEE Trans. Control Netw. Syst.*, vol. 10, no. 4, pp. 2165–2177, 2023.

[22] K. Zhang, Z. Li, Y. Wang, A. Louati, and J. Chen, "Privacy-preserving dynamic average consensus via state decomposition: Case study on multi-robot formation control," *Automatica*, vol. 139, p. 110182, 2022.

[23] Y.-W. Chen, R. Pasupathy, and J. A. Awan, "Optimal survey design for private mean estimation," *arXiv preprint arXiv:2501.18121*, 2025.

[24] G. Wang, B. Wang, T. Wang, A. Nika, H. Zheng, and B. Y. Zhao, "Defending against Sybil devices in crowdsourced mapping services," in *Proc. Annu. Int. Conf. Mob. Comput. Netw. MOBICOM*, pp. 179–191, 2016.

[25] D. P. Spanos, R. Olfati-Saber, and R. M. Murray, "Distributed sensor fusion using dynamic consensus," in *IFAC World Congress*, Citeseer, 2005.

[26] Y. Wang and P. M. Djurić, "Distributed bayesian estimation of linear models with unknown observation covariances," *IEEE Trans. on Signal Process.*, vol. 64, no. 8, pp. 1962–1971, 2015.

[27] Y. Wang, S. Mitra, and G. E. Dullerud, "Differential privacy and minimum-variance unbiased estimation in multi-agent control systems," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 9521–9526, 2017.
[28] F. Koufogiannis, S. Han, and G. J. Pappas, "Computation of privacy-preserving prices in smart grids," in *Proc. IEEE Conf. Decis. Control*, pp. 2142–2147, IEEE, 2014.
[29] H. Bai, R. A. Freeman, and K. M. Lynch, "Robust dynamic average consensus of time-varying inputs," in *Proc. IEEE Conf. Decis. Control*, pp. 3104–3109, IEEE, 2010.
[30] R. A. Freeman, P. Yang, and K. M. Lynch, "Stability and convergence properties of dynamic average consensus estimators," in *Proc. IEEE Conf. Decis. Control*, pp. 338–343, IEEE, 2006.
[31] S. S. Kia, B. Van Scoy, J. Cortes, R. A. Freeman, K. M. Lynch, and S. Martinez, "Tutorial on dynamic average consensus: The problem, its applications, and the algorithms," *IEEE Control Syst.*, vol. 39, no. 3, pp. 40–72, 2019.
[32] P. Paritosh and L. Kaplan, "Privacy-preserving convergent dynamic average consensus via state decomposition," in *IEEE Stat. Signal Process. Workshop*, 2025.
[33] B. Gharesifard and J. Cortés, "When does a digraph admit a doubly stochastic adjacency matrix?," in *Proc. Amer. Control Conf.*, pp. 2440–2445, IEEE, 2010.
[34] X. Chen, L. Huang, K. Ding, S. Dey, and L. Shi, "Privacy-preserving push-sum average consensus via state decomposition," *IEEE Trans. Autom. Control*, vol. 68, no. 12, pp. 7974–7981, 2023.
[35] S. Chatterjee and E. Seneta, "Towards consensus: Some convergence theorems on repeated averaging," *J. Appl. Probab.*, vol. 14, no. 1, pp. 89–97, 1977.
[36] J. Tsitsiklis, D. Bertsekas, and M. Athans, "Distributed asynchronous deterministic and stochastic gradient optimization algorithms," *IEEE Trans. Autom. Control*, vol. 31, no. 9, pp. 803–812, 1986.
[37] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 215–233, 2007.
[38] H. Khalil, *Nonlinear Systems*. Prentice Hall, 2002.
[39] A. Nedić and A. Olshevsky, "Distributed optimization over time-varying directed graphs," *IEEE Trans. on Autom. Control*, vol. 60, no. 3, pp. 601–615, 2014.
[40] P. Rigollet and J.-C. Hütter, "High-dimensional statistics," *arXiv preprint arXiv:2310.19244*, 2023.

Parth Paritosh is currently a Postdoctoral Fellow with Research Associateship Program at the U.S. Army Combat Capabilities DEVCOM Army Research Laboratory. He earned his Ph.D. from the Mechanical and Aerospace Engineering Department at the University of California, San Diego (UCSD). He obtained his M.S. in Mechanical Engineering from Purdue University in May 2017 and his B.Tech. in Mechanical Engineering with a minor in Computer Science and Engineering in May 2015. His research focuses on enhancing resilience in distributed estimation algorithms, particularly in multi-agent autonomous systems.

Lance M. Kaplan (Fellow, IEEE) received the B.S. degree with distinction from Duke University, Durham, NC, in 1989 and the M.S. and Ph.D. degrees from the University of Southern California, Los Angeles, in 1991 and 1994, respectively, all in Electrical Engineering. From 1987-1990, Dr. Kaplan worked as a Technical Assistant at the Georgia Tech Research Institute. He held a National Science Foundation Graduate Fellowship and a USC Dean's Merit Fellowship from 1990-1993 and worked as a Research Assistant in the Signal and Image Processing Institute at the University of Southern California from 1993-1994. Then, he worked on staff in the Reconnaissance Systems Department of the Hughes Aircraft Company from 1994-1996. From 1996-2004, he was a member of the faculty in the Department of Engineering and a senior investigator in the Center of Theoretical Studies of Physical Systems (CTSPS) at Clark Atlanta University (CAU), Atlanta, GA. Currently, he is a team leader in the Context Aware Processing branch of the US Army DEVCOM Army Research Laboratory (ARL). Previously, he served as VP Publications for the IEEE Aerospace and Electronic Systems (AES) Society (2021-2023), as Editor-In-Chief for the IEEE Transactions on AES (2012-2017), and on the Board of Governors for the IEEE AES Society (2008-2013, 2018-2020). He also served as VP Conferences for the International Society of Information Fusion (ISIF) (2014-2026) and on the Board of Directors of ISIF (2012-2014). He is a three-time recipient of the Clark Atlanta University Electrical Engineering Instructional Excellence Award from 1999-2001. He is a Fellow of ARL, ISIF, and the Military Sensing Symposia. His current research interests include information/data fusion, reasoning under uncertainty, network science, resource management and signal and image processing.

Supplementary material for Privacy-Preserving Distributed Maximum Likelihood Estimation via State Decomposition

Parth Paritosh, *Member, IEEE,* and Lance Kaplan, *Fellow, IEEE*

APPENDIX A
TECHNICAL LEMMAS

Proof [Lemma 1] Since the self loop weight $a_{ii} < 1$ in a connected network, the combined matrix A_c is doubly stochastic for $\zeta \in (0, \min\{a_{ii} | \forall i \in \mathcal{V}\})$. To compute the eigenvalues of the matrix A_c, we relate its characteristic equation to that of the matrix A using Schur complement. We can confirm that $1-\zeta$ is not an eigenvalue of A_c, as it leads to a zero eigenvector. With $\det((1-\lambda_c-\zeta)\mathbb{I}_n) \neq 0$, we can express,

$$\det(A_c - \lambda_c \mathbb{I}_{2n}) = \det((1-\lambda_c-\zeta)\mathbb{I}_n) \det\left(A - \left((\lambda_c+\zeta) + \frac{\zeta^2}{1-(\lambda_c+\zeta)}\right)\mathbb{I}_n\right).$$

The eigenvalues of the combined matrix are given as the solutions to the quadratic equation as

$$\lambda_c^{\pm}(\lambda) = \frac{(1+\lambda) \pm \sqrt{(1-\lambda)^2 + 4\zeta^2}}{2} - \zeta,$$

with $\lambda_c^+ = 1$ when $\lambda = 1$. In addition, since the corresponding gradients are given as $\frac{d}{d\lambda}\lambda_c^{\pm} = \frac{1}{2}(1 \mp \frac{1-\lambda}{\sqrt{(1-\lambda)^2+4\zeta^2}})$ are positive due to $|\frac{1-\lambda}{\sqrt{(1-\lambda)^2+4\zeta^2}}| \leq 1$, we conclude that the eigenvalues $\lambda_c^{\pm}$ increase with increasing λ. With the monotonicity of both λ_c^-, λ_c^+ and $\lambda_c^+(\lambda) > \lambda_c^-(\lambda)$, the magnitude of the second largest eigenvalue of the symmetric matrix A_c is described in terms of second largest eigenvalue $\lambda_2(A)$ as $|\lambda_2(A_c)| = \max\{|\lambda_c^+(\max_i\{\lambda_i(A)|\lambda_i(A) \neq 1\})|, |\lambda_c^-(\min_i\{\lambda_i(A)\})|\}$.

To verify that the calculated eigenvalues lie in $(-1, 1)$, we proceed by showing that $-1 < \lambda_c^- < \lambda_c^+ \leq 1$. Using Gershgorin disks, we have $\lambda(A) \geq 2a_{ii} - 1$. Along with $\zeta < a_{ii}$, this lower bounds the λ_c^- as,

$$\frac{(1+\lambda(A)) - \sqrt{(1-\lambda(A))^2 + 4\zeta^2}}{2} - \zeta \geq \frac{-\sqrt{(1-\lambda(A))^2+4\zeta^2}}{2} \geq -\sqrt{(1-a_{ii})^2 + a_{ii}^2} \geq -1.$$

The positivity of $\frac{1-\lambda}{2}$ for $\lambda \in (-1, 1]$ implies $\sqrt{(\frac{1-\lambda}{2})^2 + \zeta^2} \leq \frac{1-\lambda}{2} + \zeta$, which upper bounds λ_c^+ by 1 with equality holding only for $\lambda = 1$.

The authors are with the U.S. Army Combat Capabilities Development Command Army Research Laboratory (DEVCOM ARL), Adelphi, Maryland, pparitos@ucsd.edu, lance.m.kaplan.civ@army.mil. Research was sponsored by the Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF24-2-0101.

Manuscript received ...

Since $\sqrt{\left(\frac{1-\lambda}{2}\right)^2 + \zeta^2}$ is greater than either of its components $\frac{1-\lambda}{2}$ or ζ, and $\frac{1-\lambda}{2} > 0$, we have $\lambda_c^+(\lambda) \geq \lambda \geq \lambda_c^-(\lambda)$. Therefore, we have $\lambda_c^+(\lambda_2(A)) > \lambda_2(A)$ if $\lambda_2(A) \geq 0$ and $|\lambda_c^-(\lambda_2(A))| > |\lambda_2(A)|$ otherwise, implying that the second eigenvalue of matrix A_c is greater than that of matrix A. ■

Lemma S1. *Let the sequence of matrices $\Sigma_t \in \mathbb{R}^{d\times d}$ converge to a p.d. matrix $\Sigma^\star$ as $\|\Sigma_t - \Sigma^\star\|_F \leq a_t$, where a_t is a vanishing sequence. Then, the sequence of inverses satisfy $\|\Sigma_t^{-1} - (\Sigma^\star)^{-1}\|_F \leq \frac{a_t\sqrt{d}\|(\Sigma^\star)^{-1}\|_F}{\sigma_{\min}(\Sigma^\star) - a_t}$.*

Proof Using triangle inequality on Frobenius norm, we have $\|\Sigma^\star\|_F \leq \|\Sigma_t\|_F + \frac{c}{\sqrt{t}}$. Since the rank of the square matrix Σ_t is bounded by its dimension d,

$$\|\Sigma_t^{-1}\|_F \leq \sqrt{d}\|\Sigma_t^{-1}\|_2 = \sqrt{d}\max_{\|x\|\neq 0}\frac{\|\Sigma_t^{-1}x\|_2}{\|x\|_2} = \sqrt{d}\left(\min_{\|y\|\neq 0}\frac{\|\Sigma_t y\|_2}{\|y\|_2}\right)^{-1} = \frac{\sqrt{d}}{\sigma_{\min}(\Sigma_t)} \leq \frac{\sqrt{d}}{\sigma_{\min}(\Sigma^\star) - a_t},$$

where the upper bound on $\sigma_{\min}(\Sigma_t)^{-1}$ follows from [*S1*, Corollary 7.3.5]. Here, we use $|\sigma_{\min}(\Sigma_t) - \sigma_{\min}(\Sigma^\star)| \leq \|\Sigma_t - \Sigma^\star\|_2 \leq \|\Sigma_t - \Sigma^\star\|_F$. Next, we use the relation $\Sigma_t^{-1} - (\Sigma^\star)^{-1} = \Sigma_t^{-1}(\Sigma^\star - \Sigma_t)(\Sigma^\star)^{-1}$ and bound individual terms to prove the result. ■

The general result explains the rate of convergence of the information matrices given the properties of covariance estimates in Lemma 3.

Lemma S2. *The sequence of information matrices $\Omega_{i,t} \in \mathbb{R}^{d\times d}$ converge to a p.d. matrix $\Omega_i^\star$ for $a_t = \|\Sigma_i^\star\|_{op}\sqrt{\frac{d+\log(1/\delta)}{t}}$ as $\mathbb{P}\left(\|\Omega_{i,t} - \Omega_i^\star\|_F \leq \frac{a_t\sqrt{d}\|(\Omega^\star)^{-1}\|_F}{\sigma_{\min}(\Omega^\star) - a_t}\right) \geq 1-\delta$.*

Proof Since d is the dimensionality and maximum rank of the covariance matrix, we have $\|\Sigma\|_{op} \leq \|\Sigma\|_F \leq \sqrt{d}\|\Sigma\|_{op}$. We use it to express the bound in Lemma 3 in terms of Frobenius norm and then apply Lemma S1 to conclude the claim. ■

Since the lemma holds for sufficiently large time steps t, we can bound the difference between consecutive estimates as,

Lemma S3. *For some $c > 0$, the change in empirical information means satisfy $\|\Omega_{i,t+1}\beta_{i,t+1} - \Omega_{i,t}\beta_{i,t}\|_F \leq c/\sqrt{t}$ w.p. at least $(1-\delta)$.*

Proof We use the convergence of the local information matrix as $\|\Omega_{i,t}-\Omega_i^\star\|_F \leq c_1/\sqrt{t}$ and mean as $\|\beta_{i,t}-\mu^\star\|_F \leq c_2/\sqrt{t}$. Simplifying with $\Omega_{i,t}\mu^\star$ and applying triangle inequality,

$$\|\Omega_{i,t}\beta_{i,t} - \Omega_i^\star\mu^\star\|_2 \leq (\|\Omega_i^\star\|_F + \|\Omega_{i,t}-\Omega_i^\star\|_F)\|\beta_{i,t}-\mu^\star\|_2 + \|\Omega_{i,t}-\Omega_i^\star\|_F\|\mu^\star\|_2 \leq c_1c_2/t + c_3/\sqrt{t}.$$

For sufficiently large $t>0$, we simplify with $\Omega_i^\star\mu^\star$ to show that the change in information mean is bounded above as $\|\Omega_{i,t+1}\beta_{i,t+1} - \Omega_{i,t}\beta_{i,t}\|_F \leq c_4/\sqrt{t}$. Since the upper bounds are a logical implication of existing statement w.p. at least $(1-\delta)$, the same probabilistic lower bound holds. ∎

Lemma S4. *The sum $S_t = \sum_{k=1}^t \frac{\lambda^{t-k}}{k^\alpha}$, with $\alpha>0$ and $\lambda\in(0,1)$ is bounded above for any sufficiently large $t > t_0 = \lceil \frac{\lambda^{1/\alpha}}{1-\lambda^{1/\alpha}} \rceil$ as $S_t < ct^{-\alpha}$ for some $c>0$.*

Proof We first express the series as an iterative update,

$$S_{t+1} = \lambda S_t + (t+1)^{-\alpha}.$$

For the initial condition $S_1=1$, the solution to this difference equation is deduced as linear combination of solutions to the homogenous and non-homogenous parts. The general solution of the homogenous part given by the geometric series $S_{t+1} = \lambda S_t$ is $c_1\lambda^{t-1}$ for some constant $c_1>0$.

Any particular solution to the non-homogenous difference equation satisfies $S_t^{(p)} = \lambda S_{t-1}^{(p)} + \frac{1}{t^\alpha}$. Upon taking a method of variations approach, we can show that the particular solution is arbitrarily close to $\frac{1}{(1-\lambda)t^\alpha}$. To do this, we assume the following form for solution and express the update as,

$$S_t^{(p)} = c_{1,t}\lambda^{t-1} + c_{2,t}\frac{1}{(1-\lambda)t^\alpha}.$$

$$c_{1,t+1}\lambda^t + \frac{c_{2,t+1}}{(1-\lambda)(t+1)^\alpha} = c_{1,t}\lambda^t + \frac{\lambda c_{2,t}}{(1-\lambda)t^\alpha} + \frac{1}{(t+1)^\alpha}.$$

$$\implies c_{1,t+1} = c_{1,t} = c_1, c_{2,t+1} = \lambda((t+1)/t)^\alpha c_{2,t} + (1-\lambda).$$

Since $S_1=1$, the constant $c=1$ and $c_{2,1}=0$. Since $\alpha>0$, the rate coefficient $\bar\lambda(t) = \lambda\left(\frac{t+1}{t}\right)^\alpha$ satisfies,

$$\bar\lambda(t) > \lambda,\ \bar\lambda(t+1) < \bar\lambda(t),\ \forall t\in\mathbb{Z}_{\geq 0}.$$

The time step $t_0>0$ for which the rate coefficient is strictly bounded above as,

$$\bar\lambda(t_0) < 1, \text{ if } t_0 = \left\lceil \frac{\lambda^{1/\alpha}}{1-\lambda^{1/\alpha}} \right\rceil.$$

For any time $t > t_0$, the term $\lambda((t+1)/t)^\alpha < 1$ and monotonically decreasing. Therefore, we can choose a sharper rate coefficient at a time step $t_1 \geq t_0$ to upper and lower bound the updates at all $t > t_1$ as,

$$\lambda c_{2,t} + (1-\lambda) < c_{2,t+1} < \bar\lambda(t_1)c_{2,t} + (1-\lambda),$$

where we choose $\bar\lambda(t_1) = \lambda\left(\frac{t_1+1}{t_1}\right)^\alpha \in (0,1)$ in the upper bound arbitrarily close to λ. Since the updates on the bounds match a geometric series, we express the lower bound as,

$$c_{2,t+1} > \lambda^{t-t_1}c_{2,t_1} + \sum_{k=1}^{t-t_1}\lambda^{k-1}(1-\lambda) = \lambda^{t-t_1}c_{2,t_1} + 1 - \lambda^{t-t_1}.$$

The upper bound is based on decreasing rate coefficient as,

$$\begin{aligned} c_{2,t+1} &< \bar\lambda(t_1)^{t-t_1}c_{2,t_1} + \sum_{k=1}^{t-t_1}\bar\lambda(t_1)^{k-1}(1-\lambda) \\ &< \bar\lambda(t_1)^{t-t_1}c_{2,t_1} + \frac{(1-\lambda)}{1-\bar\lambda(t_1)}. \qquad \text{(Since } \bar\lambda(t_1)<1\text{)} \end{aligned}$$

For the initialization, the solution can thus be expressed as,

$$S_t < \lambda^{t-1} + \frac{\bar\lambda(t_1)^{t-t_1}}{(1-\lambda)t^\alpha}c_{2,t_1} + \frac{1}{1-\bar\lambda(t_1)}\cdot\frac{1}{t^\alpha}.$$

Since λ^t converges faster than $t^{-\alpha}$, the term S_t is bounded above for sufficiently large $t>0$ and some constant $c(\lambda)$ as $S_t < ct^{-\alpha}$. ∎

APPENDIX B
CONVERGENCE PROOFS

Proof [Thm. 4] We begin by observing that the information mean updates as a linear system with stochastic inputs. To do this, define a vector of all public and private estimates as,

$$\boldsymbol{\nu}_t = [(\nu_{1,t}^a)^\top, \cdots, (\nu_{n,t}^a)^\top, (\nu_{1,t}^s)^\top, \cdots, (\nu_{n,t}^s)^\top]^\top \in \mathbb{R}^{2nd}.$$

We similarly define the vector of public and private inputs as $u_t = [(x_{1,t}^\nu)^\top, \cdots, (x_{n,t}^\nu)^\top, (y_{n,t}^\nu)^\top, \cdots, (y_{n,t}^\nu)^\top]^\top$, and denote their rth vector components as $\boldsymbol{\nu}_{r,t}, u_{r,t} \in \mathbb{R}^d$ for $r\in\{1,\ldots,2n\}$. Iteratively substituting the prior inputs,

$$\boldsymbol{\nu}_{r,t+1} = \sum_{j_1=1}^{2n}[A_c^t]_{rj_1}\boldsymbol{\nu}_{j_1,1} + \sum_{k=1}^{t}\sum_{j_1=1}^{2n}[A_c^{t-k}]_{rj_1}u_{j_1,k}. \tag{S1}$$

From Lemma 2, each element $[A_c^{t-k}]_{rj_1} = 1/2n + \gamma_{rj_1}^{t,k}$ with error bound $|\gamma_{rj_1}^{t,k}| \leq \lambda_c^{t-k}$ and input sums satisfying $\sum_{j_1=1}^{2n}u_{j_1,k} = 2\sum_{j=1}^n\Omega_j^\star(\beta_{j,k+1}-\beta_{j,k})$, we get,

$$\begin{aligned} \boldsymbol{\nu}_{r,t+1} =& \frac{1}{2n}\sum_{j_1=1}^{2n}\boldsymbol{\nu}_{j_1,1} + \frac{1}{n}\sum_{j=1}^n\sum_{k=1}^t\Omega_j^\star(\beta_{j,k+1}-\beta_{j,k}) \\ &+ \underbrace{\sum_{j_1=1}^{2n}\gamma_{rj_1}^{t,0}\boldsymbol{\nu}_{j_1,1}}_{V_2} + \underbrace{\sum_{k=1}^t\sum_{j_1=1}^{2n}\gamma_{rj_1}^{t,k}u_{j_1,k}}_{V_3}, \end{aligned} \tag{S2}$$

where the initialization condition implies that $\sum_{j_1=1}^{2n}\boldsymbol{\nu}_{j_1,1} = 2\sum_{j=1}^n\Omega_j^\star\beta_{j,1}$. Let the adjusted information mean $\bar{\boldsymbol{\nu}}_{r,t+1}$ w.r.t. the true information mean $\nu^\star = \frac{1}{n}\sum_{j=1}^n\Omega_j^\star\mu^\star$ be,

$$\bar{\boldsymbol{\nu}}_{r,t+1} = \boldsymbol{\nu}_{r,t+1} - \nu^\star = V_1 + V_2 + V_3, \tag{S3}$$

where V_1 is computed by simplifying the telescoping series with terms $\sum_{j=1}^n\Omega_j^\star\beta_{j,k}$ for $k\leq t$ in (S2),

$$V_1 = \frac{1}{n}\sum_{j=1}^n\Omega_j^\star\beta_{j,t+1} - \nu^\star = \frac{1}{n}\sum_{j=1}^n\Omega_j^\star\bar\beta_{j,t+1},$$

with adjusted local mean $\bar\beta_{i,k} = \beta_{i,k} - \mathbb{E}[\beta_{i,k}] = \beta_{i,k} - \mu^\star$.

To bound the deviation from true information mean value, we need to compute the expected norm error as,

$$\begin{aligned} \mathbb{E}[\|\bar{\boldsymbol{\nu}}_{r,t+1}\|_2^2] =& \mathbb{E}[V_1^\top V_1 + V_2^\top V_2 + V_3^\top V_3 \\ &+ 2V_1^\top V_2 + 2V_2^\top V_3 + 2V_1^\top V_3]. \end{aligned} \tag{S4}$$

We compute the expectation by expressing the initial estimates $\nu_{j_1,1}$ in V_2 and input components $u_{j_1,k}$ in V_3 as a linear combination of the local means $\beta_{j_1,k}$, whose moments are known. The initial information mean is written in terms of the local ones as $\nu_{i,0} = F_i^a \Omega_i^\star \beta_{i,1}$ for $i \in \{1,\dots,n\}$ and $\nu_{i,0} = F_i^s \Omega_i^\star \beta_{i-n,1}$ for the remaining $i \in \{n+1,\cdots,2n\}$, where the matrices F_i^a and F_i^s are bounded and sum to identity. After mixing with bounded matrices $B^\nu, \mathcal{B}^\nu$ in (32), the information mean can be expressed as a linear update of local means $\beta_{i,1}$ with bounded matrices $\|F_{i,\ell}\| \le M_1$ as,

$$\nu_{i,1} = \sum_{\ell=1}^{n} F_{i,\ell}\Omega_\ell^\star \beta_{\ell,1} = \sum_{\ell=1}^{n} F_{i,\ell}\Omega_\ell^\star(\bar\beta_{\ell,1} + \theta^\star),$$
$$F_{i,\ell} = \begin{cases} (B_{\ell\ell} - \mathcal{B}_\ell)F_\ell^a + \mathcal{B}_\ell F_\ell^s & \text{if } i = \ell,\ i \le n, \\ B_{i\ell}F_\ell^a & \text{if } i \ne \ell,\ i \le n, \\ \mathcal{B}_\ell(F_\ell^a - F_\ell^s) & \text{if } i - n = \ell,\ i > n, \\ 0 & \text{otherwise.} \end{cases} \tag{S5}$$

This allows us to express the term V_2 in (S3) as,

$$\begin{aligned} V_2 &= \sum_{j_1=1}^{2n} \gamma_{rj_1}^{t,0} \left(\sum_{\ell=1}^{n} F_{j_1,\ell}\Omega_\ell^\star(\bar\beta_{\ell,1} + \theta^\star) \right) \\ &= \sum_{\ell=1}^{n}\sum_{j_1=1}^{2n} \gamma_{rj_1}^{t,0} F_{j_1,\ell}\Omega_\ell^\star \bar\beta_{\ell,1} + \sum_{j_1=1}^{2n}\sum_{\ell=1}^{n} \gamma_{rj_1}^{t,0} F_{j_1,\ell}\Omega_\ell^\star\theta^\star. \end{aligned} \tag{S6}$$

For $j_1 \in \{1,\dots,n\}$, the norm of inputs after (33) is bounded for a positive definite $\Omega_i^\star$ as $\|u_{j_1,k}\| \le M\|\Omega_i^\star(\beta_{j_1,k+1} - \beta_{j_1,k})\|$, and there exists $D_{j_1,k} \in \mathbb{R}^{d\times d}$ such that $u_{j_1,k} = D_{j_1,k}\Omega_{j_1}^\star(\beta_{j_1,k+1} - \beta_{j_1,k})$, with $\|D_{j_1,k}\| \le M$. Similarly, there exists $D_{j_1,k}$ satisfying $\|D_{j_1,k}\| \le M$ in $j_1 \in \{n,\cdots,2n\}$,

$$u_{j_1,k} = D_{j_1,k}\Omega_{j_1-n}^\star(\beta_{j_1-n,k+1} - \beta_{j_1-n,k}). \tag{S7}$$

Corresponding to agent $j \in \mathcal{V}$, the matrix multipliers to the inputs satisfy $D_{j,k} + D_{j+n,k} = 2\mathbb{I}_d$. Simplifying with the expected value $\mu^\star$, we can express $u_{j_1,k} = D_{j_1,k}\Omega_{j_1}^\star(\bar\beta_{j_1,k+1} - \bar\beta_{j_1,k})$ with $\mathbb{E}[u_{j_1,k}] = 0$ to use the results in Lemma 6.

We will now compute the expected value over the six terms in (S4). Applying Lemma 6 to the first term,

$$\begin{aligned} \mathbb{E}[V_1^\top V_1] &= \frac{1}{n^2}\sum_{j=1}^{n} \mathbb{E}[\bar\beta_{j,t+1}^\top(\Omega_j^\star)^\top\Omega_j^\star\bar\beta_{j,t+1}] \\ &= \frac{1}{(t+1)n^2}\sum_{j=1}^{n} \mathrm{tr}[(\Omega_j^\star)^\top\Omega_j^\star\Sigma_j^\star] = \frac{1}{(t+1)n}\left(\frac{1}{n}\sum_{j=1}^{n}\mathrm{tr}(\Omega_j^\star)\right). \end{aligned}$$

Substituting (S6) into the second term in (S4), using the independence across agents and expectation $\mathbb{E}[\bar\beta_{\ell,1}] = 0$,

$$\begin{aligned} \mathbb{E}[V_2^\top V_2] &= \left\| \sum_{j_1=1}^{2n}\sum_{\ell=1}^{n} \gamma_{rj_1}^{t,0} F_{j_1,\ell}\Omega_\ell^\star\theta^\star \right\|^2 \\ &+ \sum_{\ell=1}^{n} \mathbb{E}\Big[\bar\beta_{\ell,1}^\top(\Omega_\ell^\star)^\top \Big(\sum_{j_1=1}^{2n} \gamma_{rj_1}^{t,0} F_{j_1,\ell}^\top\Big)\Big(\sum_{j_2=1}^{2n} \gamma_{rj_2}^{t,0} F_{j_2,\ell}\Big)\Omega_\ell^\star\bar\beta_{\ell,1}\Big] \\ &= \left\| \sum_{j_1=1}^{2n}\sum_{\ell=1}^{n} \gamma_{rj_1}^{t,0} F_{j_1,\ell}\Omega_\ell^\star\theta^\star \right\|^2 \\ &+ \sum_{\ell=1}^{n}\sum_{j_1=1}^{2n}\sum_{j_2=1}^{2n} \gamma_{rj_1}^{t,0}\gamma_{rj_2}^{t,0}\,\mathrm{tr}((\Omega_\ell^\star)^\top F_{j_1,\ell}^\top F_{j_2,\ell}). \end{aligned}$$

Since $|\gamma_{rj_1}^{t,0}| \le \lambda_c^t$ and bounded $\|F_{j,\ell}\| \le M_1$, we upper bound the quadratic term with some $c_{22} > 0$ as,

$$\implies |\mathbb{E}[V_2^\top V_2]| \le c_{22}\lambda_c^{2t}.$$

Let us now focus on the cross terms in (S4). Using the independence across agents and zero mean of $\bar\beta_{\ell,1}$,

$$\begin{aligned} \mathbb{E}[V_1^\top V_2] &= \frac{1}{n}\mathbb{E}\Big[\sum_{j=1}^{n} \bar\beta_{j,t+1}^\top(\Omega_j^\star)^\top \Big(\sum_{j_1=1}^{2n} \gamma_{rj_1}^{t,0} F_{j_1,j}\Big)\Omega_j^\star\bar\beta_{j,1}\Big] \\ &= \frac{1}{n}\sum_{j=1}^{n} \frac{\mathrm{tr}((\Omega_j^\star)^\top(\sum_{j_1=1}^{2n}\gamma_{rj_1}^{t,0}F_{j_1,j})\Omega_j^\star\Sigma_j^\star)}{t+1} \\ &= \frac{1}{n(t+1)}\sum_{j_1=1}^{2n}\gamma_{rj_1}^{t,0}\sum_{j=1}^{n}\mathrm{tr}((\Omega_j^\star)^\top F_{j_1,j}). \\ &\implies |\mathbb{E}[2V_1^\top V_2]| \le c_{12}\frac{\lambda_c^t}{n(t+1)}. \end{aligned}$$

Using independence across agents and time, and recalling that expected inputs differences in (S7) satisfy $\mathbb{E}[u_{j_1,k}] = 0$,

$$\begin{aligned} \mathbb{E}[V_2^\top V_3] &= \mathbb{E}\Big[\Big(\sum_{j_1=1}^{2n}\gamma_{rj_1}^{t,0}\nu_{j_1,1}^\top\Big)\Big(\sum_{k=1}^{t}\sum_{j_2=1}^{2n}\gamma_{rj_2}^{t,k}u_{j_2,k}\Big)\Big] \\ &= \mathbb{E}\Big[\Big(\sum_{\ell=1}^{n}\sum_{j_1=1}^{2n}\gamma_{rj_1}^{t,0}F_{j_1,\ell}\Omega_\ell^\star\bar\beta_{\ell,1}\Big)^\top\Big(\sum_{k=1}^{t}\sum_{j_2=1}^{2n}\gamma_{rj_2}^{t,k}u_{j_2,k}\Big)\Big] \\ &= \sum_{k=1}^{t}\sum_{j=1}^{n}\mathbb{E}\Bigg[\gamma_{rj}^{t,k}\bar\beta_{j,1}^\top(\sum_{j_1=1}^{2n}\gamma_{rj_1}^{t,0}\Omega_j^\star F_{j_1,j})^\top D_{j,k}\Omega_j^\star(\bar\beta_{j,k+1} - \bar\beta_{j,k}) \\ &\quad + \gamma_{r,j+n}^{t,k}\bar\beta_{j,1}^\top(\sum_{j_1=1}^{2n}\gamma_{rj_1}^{t,0}\Omega_j^\star F_{j_1,j})^\top D_{j+n,k}\Omega_j^\star(\bar\beta_{j,k+1} - \bar\beta_{j,k})\Bigg] \\ &= \sum_{k=1}^{t}\sum_{j=1}^{n}\Bigg[\gamma_{rj}^{t,k}\,\mathrm{tr}\left((\sum_{j_1=1}^{2n}\gamma_{rj_1}^{t,0}\Omega_j^\star F_{j_1,j})^\top D_{j,k}\right)\cdot\frac{-1}{k(k+1)} \\ &\quad + \gamma_{r,j+n}^{t,k}\,\mathrm{tr}\left((\sum_{j_1=1}^{2n}\gamma_{rj_1}^{t,0}\Omega_j^\star F_{j_1,j})^\top D_{j+n,k}\right)\cdot\frac{-1}{k(k+1)}\Bigg]. \end{aligned}$$

With $\|D_{j,k}\| \le M$, $\|F_{j_1,j}\| \le M_1$ for all $j \in \{1,\dots,n\}, j_1 \in \{1,\dots,2n\}$ and $k > 0$, we have for some $c > 0$,

$$|\mathbb{E}[V_2^\top V_3]| \le c_{23}\lambda_c^t\sum_{k=1}^{t}\frac{\lambda_c^{t-k}}{k^2} \le c_{23}\frac{\lambda_c^t}{t^2}.$$

Substituting the local mean differences from (S7) into V_3, and simplifying with Lemma 6, we have,

$$V_3^\top V_3 = \sum_{k=1}^{t}\sum_{j_1=1}^{2n} (\gamma_{rj_1}^{t,k})^2 \mathbb{E}[u_{j_1,k}^\top u_{j_1,k}]. \tag{S8}$$

Now, we consider the expectation as,

$$\begin{aligned}\mathbb{E}[u_{j_1,k}^\top u_{j_1,k}] &= \mathbb{E}[\|D_{j_1,k}\Omega_{j_1}^\star(\bar\beta_{j_1,k+1}-\bar\beta_{j_1,k})\|^2]\\ &= \frac{\operatorname{tr}((\Omega_{j_1}^\star)^\top D_{j_1,k}^\top D_{j_1,k})}{k(k+1)}.\end{aligned}$$

Since $|\gamma_{rj_1}^{t,k}| \le \lambda_c^{t-k}$ and bounded $\|D_{j_1,k}\| \le M$, we upper bound the absolute quadratic term as,

$$|\mathbb{E}[V_3^\top V_3]| \le \sum_{k=1}^{t} \lambda_c^{2(t-k)} \cdot \frac{2M^2\sum_{j=1}^n \operatorname{tr}(\Omega_{j_1}^\star)}{k(k+1)}.$$

For a sufficiently large time t, Lemma 4 implies that,

$$\sum_{k=1}^{t}\frac{\lambda_c^{2(t-k)}}{k(k+1)} \le \sum_{k=1}^{t}\frac{\lambda_c^{2(t-k)}}{k^2} \le \frac{1}{t^2}.$$

As a result, $|\mathbb{E}[V_3^\top V_3]| \le c_{33}/t^2$ for some $c_{33}>0$.

Finally, with the simplification using the independence in Assumption 1 and computing expectation with Lemma 6,

$$\begin{aligned}V_1^\top V_3 &= \frac{1}{n}\sum_{k=1}^{t}\sum_{j=1}^{n}\mathbb{E}\Big[\bar\beta_{j,t+1}^\top(\Omega_j^\star)^\top\Big(\sum_{j_1=1}^{2n}\gamma_{rj_1}^{t,k}u_{j_1,k}\Big)\Big]\\
&= \frac{1}{n}\sum_{k=1}^{t}\sum_{j=1}^{n}\mathbb{E}\Big[(\gamma_{rj}^{t,k}\bar\beta_{j,t+1}^\top(\Omega_j^\star)^\top D_{j,k}\Omega_j^\star(\bar\beta_{j,k+1}-\bar\beta_{j,k})\\
&\quad +\gamma_{r,j+n}^{t,k}\bar\beta_{j,t+1}^\top(\Omega_j^\star)^\top D_{j+n,k}\Omega_j^\star(\bar\beta_{j,k+1}-\bar\beta_{j,k}))\Big]\\
&= \frac{1}{n}\sum_{k=1}^{t}\sum_{j=1}^{n}\left(\gamma_{rj}^{t,k}\operatorname{tr}((\Omega_j^\star)^\top D_{j,k})\left(\frac{1}{t+1}-\frac{1}{t+1}\right)\right.\\
&\quad \left.+\gamma_{r,j+n}^{t,k}\operatorname{tr}((\Omega_j^\star)^\top D_{j,k})\left(\frac{1}{t+1}-\frac{1}{t+1}\right)\right)=0.\end{aligned}$$

where the last step follows due to positive definiteness of $\Omega_j^\star$. Compiling the upper bound with $c_j = \operatorname{tr}(\Omega_j^\star)$,

$$\mathbb{E}[\|\bar{\mathbf{v}}_{r,t+1}\|_2^2] \le \frac{\frac{1}{n}\sum_{j=1}^n c_j}{(t+1)n} + c_{22}\lambda_c^{2t} + \frac{c_{33}}{t^2} + \frac{c_{12}\lambda_c^t}{n(t+1)} + c_{23}\frac{\lambda_c^t}{t^2}.$$

■

APPENDIX C
PRIVATE GENERATION OF INITIAL WEIGHTS

The selection of the inter-agent weights B_{ij} in (9) requires coordination to satisfy the column sum constraint. In an undirected network, this constraint restricts coordination to the neighbor set at each agent. While similar weight constraints appear in [*S2*, *S3*], these works do not address their private generation. For each agent j, we assume that each of its neighbors generate a matrix B_{ij}. Then, we have to securely compute $B_{jj} = \mathbb{I}_d - \sum_{i\in\mathcal{V}_j} B_{ij}$ at the agent j without revealing any of the components.

Due to the connectivity assumption in conjunction with the cardinality constraint $|\mathcal{V}| > 2$, the sole neighbor of a leaf node j is not a leaf node. Therefore, even though the node j accesses the column weights corresponding to the column containing B_{jj}, they do not access all the weights $\{B_{i\ell}\}$ of the neighbor i. This preserves the privacy w.r.t. the leaf node j. Therefore, we now consider the weight generation in columns corresponding to agents with more than one neighbor. For their distributed generation, we consider the homomorphic encryption approach as detailed below:

Homomorphic Encryption: Let the neighbors of agent j be given as $j_1,\dots,j_{n_j}$. Since the network is connected with more than two nodes, the number of neighbors at agent j satisfies $n_j \ge 2$, implying that $j_1 \ne j_{n_j}$. Next, we show how to use the additive homomorphism property of the Paillier cryptosystem [*S4*] to design a secure aggregation algorithm for distributed generation of feasible inter-agent weights. Please see [*S5*] for more details on public and private key generation and [*S6*] for an application towards privacy preserving static-consensus algorithms. The algorithm proposed for securely generating inter-agent weights is given as:

1) Agent j designates neighbor j_1 for generating encryption keys. Agent j_1 generates public and private keys given as kp_{j_1} and ks_{j_1}.
2) Agent j_1 shares the public key kp_{j_1} and corresponding encrypted weight $E(B_{j_1 j})$ with agent j.
3) Agent j shares the public key kp_{j_1} with all other neighbors, and receives their encrypted weights $E(B_{j_2 j}),\dots,E(B_{j_{n_j-1}j})$.
4) Agent j computes the encrypted sum by multiplying the ciphertexts as $\prod_{\ell=1}^{n_j} E(B_{j\ell j})$, and sends it to agent j_1 for decryption.
5) Agent j_1 recovers the sum $\sum_{\ell=1}^{n_j} B_{j\ell j}$ using the private key ks_{j_1} and sends it to agent j for computing weight $\mathbb{I} - \sum_{\ell=1}^{n_j} B_{j\ell j}$ satisfying the column sum constraint.

The primary intuition behind this algorithm is the separation of agent accessing the private key from the agent multiplying the encrypted weights. Since this step is implemented once, our state decomposition algorithm avoids the costs of repeatedly generating keys and accumulation of quantization errors due to the prime number based encryption.

REFERENCES

[S1] R. A. Horn and C. R. Johnson, *Matrix analysis*. Cambridge university press, 2012.

[S2] Y. Wang, "Privacy-preserving average consensus via state decomposition," *IEEE Trans. Autom. Control*, vol. 64, no. 11, pp. 4711–4716, 2019.

[S3] H. Cheng, X. Liao, H. Li, Q. Lü, and Y. Zhao, "Privacy-preserving push-pull method for decentralized optimization via state decomposition," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 10, pp. 513–526, 2024.

[S4] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International conference on the theory and applications of cryptographic techniques*. Springer, 1999, pp. 223–238.

[S5] J. Katz and Y. Lindell, *Introduction to modern cryptography: principles and protocols*. Chapman and hall/CRC, 2007.

[S6] M. Ruan, H. Gao, and Y. Wang, "Secure and privacy-preserving consensus," *IEEE Trans. Autom. Control*, vol. 64, no. 10, pp. 4035–4049, 2019.