Distributed Privacy–Preserving Iterative Summation Protocols

1st Yang Liu
Tencent Cloud Product Department
Tencent
Shenzhen, China
clarkieliu@tencent.com

2nd Qingchen Liu
Chair of Information-Oriented Control
Technical University of Munich
Munich, Germany
qingchen.liu@tum.de

3rd Xiong Zhang
Tencent Cloud Product Department
Tencent
Shenzhen, China
farleyzhang@tencent.com

4th Shuqi Qin
Tencent Cloud Product Department
Tencent
Shenzhen, China
sookieqin@tencent.com

5th Xiaoping Lei
Tencent Cloud Product Department
Tencent
Shenzhen, China
edenlei@tencent.com

***Abstract*—In this paper, we study the problem of summation evaluation of secrets. The secrets are distributed over a network of nodes that form a ring graph. Privacy–preserving iterative protocols for computing the sum of the secrets are proposed, which are resilient against dynamic node join and leave situations. Theoretic bounds are derived regarding the utility and accuracy, and the proposed protocols are shown to comply with differential privacy requirements. Based on utility, accuracy and privacy, we also provide guidance on appropriate selections of random noise parameters. Additionally, a few numerical examples that demonstrate their effectiveness and superiority are provided.**

***Index Terms*—Privacy Preservation, Secure Summation, Differential Privacy**

I. Introduction

Data mining is a practical technique to extract useful patterns from datasets. Generally, conventional data mining algorithms are developed from a centralized perspective, and effective and robust over an aggregated dataset with an implicit assumption that the collection of such a dataset is unimpeded. However, as the information technology rapidly develops, machines that manage to collect and store data, undertake computing and communication tasks are ubiquitous, from powerful servers, to personal agents, such as PCs and smart phones. On the one hand, data collection is usually carried out in a distributed fashion, the data aggregation pushes the communication and computation cost of the central server to a bottleneck on the implementation of centralized data mining methods. On the other hand, the collected data might be sensitive and confidential to the distributed agents, and therefore unanonymized plain data are prohibited to give away directly. Confronted with these challenges in terms of distributed computation and privacy preservation, improvements have to be made on existing data mining methods. The relevant field have drawn much attention [1].

The work of Q. Liu was supported by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement (754462).

The evaluation of sum of a collection of secrets is a fundamental problem that arises in the distributed privacy–preserving data mining. This topic has drawn much attention of researchers from various fields, including cryptography, computer science and control science. In the field of secure multi–party computation, efficient secure sum protocols are presented [2]. However, not only the collusion of two participating parties would compromise the secret of the one who is adjacent to both of them, but all parties must follow interaction rules in a default order in finite steps, making it fragile against the disturbance caused by node join and leave. In addition, homomorphic encryption [3] and secret sharing [4] can be used as secure summation tools. Nevertheless, the encryption of plaintext yields much more complex results in general, resulting in high communication and computational complexity. Privacy-preserving average consensus protocols [5]–[8] utilize statistical or cryptographical elements to compute network sum in a secure fashion, but few can provide satisfactory convergence accuracy with dynamic resilience unexplored.

In this paper, we aim to develop privacy–preserving summation protocols that has high accuracy, low complexity and strong resilience against dynamic disturbance. The contributions of this paper are summarized as follows.

(i) Innovative distributed privacy–preserving iteration–based protocols for evaluating summation of secrets are proposed.
(ii) Theoretic analysis on utility, accuracy and privacy is provided, in addition to further investigations on the tradeoff problem between utility, accuracy and privacy that provides guidance on the choice of random noise.
(iii) Simulations are provided, which verify the effectiveness of the proposed protocols and compare them with a few existing works to highlight the advantages in terms of accuracy, complexity and dynamic resilience.

The rest of this paper is organized as follows. The problem

formulation is introduced in Section II. We propose our protocols in Section III. Theoretic analysis of utility, accuracy and privacy is provided in Section IV. In Section V, several examples are give to demonstrate the effectiveness and superiority of the proposed protocols. A few concluding remarks are given in Section VI.

II. Problem Definition

A. Network

Let a group of nodes be indexed as in $\mathrm{V} = \{1, \ldots, n\}$ with $n > 2$. Each node $i \in \mathrm{V}$ can send information to only one of the other nodes $j \in \mathrm{V}$, with the connection represented by an ordered pair (i, j). We suppose, without loss of generality, that node i talks to node $i+1$ for $i = 1, \ldots, n-1$ and node n talks to node 1, based on which we introduce a permutation $\pi : \mathrm{V} \to \mathrm{V}$ with

$$\pi(i) = \begin{cases} i+1 & \text{if } i = 1, \ldots, n-1; \\ 1 & \text{otherwise.} \end{cases}$$

Then the network can be modelled by a directed ring graph $\mathrm{G} = (\mathrm{V}, \mathrm{E})$ illustrated in Figure 1, where the edge set $\mathrm{E} = \{(i, \pi(i)) : i \in \mathrm{V}\}$.

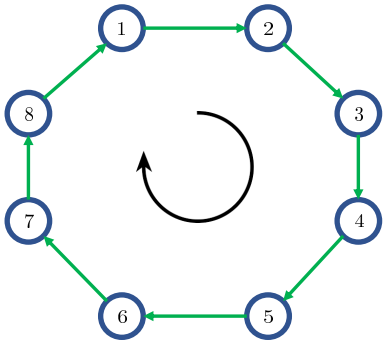


Fig. 1: An 8–node directed ring graph.

B. General Privacy–Preserving Summation Protocols

Consider a distributed summation occasion in which each node $i \in \mathrm{V}$ holds a secret $s_i \in \mathbb{R}$. The collective goal for all nodes is to compute $\sum_{i \in \mathrm{V}} s_i$ by undertaking certain communication strategies over the network G, in the meantime each node does not disclose its own secret to others. Formally, we write the principles for Privacy–Preserving Summation Protocols (PPSPs) as follows.

(i) [*Communication Principle*]: Each node $i \in \mathrm{V}$ is only permitted to interact with $\pi(i)$.

(ii) [*Privacy Principle*] Each node $i \in \mathrm{V}$ does not disclose s_i to others.

(iii) [*Utility Principle*] Each node obtains $\sum_{i \in \mathrm{V}} s_i$ as output.

III. Achievements with Iterative Method

A. The Protocol

In this section, we introduce realizations of PPSPs. We discretize the time as $k = 0, 1, 2, \ldots$. Let each node $i \in \mathrm{V}$ hold a dynamic state $x_i(k)$, initialized as $x_i(0) = s_i$. Introduce $v_i : \mathbb{Z}^{\geq 0} \to \mathbb{R}$ for all $i \in \mathrm{V}$ satisfying $\lim_{k \to \infty} v_i(k) = 0$. Let $\{\beta_i(k)\}_{i \in \mathrm{V}, k \in \mathbb{Z}^{\geq 0}}$ be independent random variables. Let π^{-1} denote the inverse of the permutation π. Then our deterministic iterative PPSP can be described as follows.

SI-PPSP Synchronous Iterative PPSP

1: Set $k \leftarrow 0$ and initialize $x_i(0) = s_i$ for all $i \in \mathrm{V}$.
2: Each node i generates $\beta_i(k) \in \mathbb{R}$ according to a distribution with zero mean and variance $v_i^2(k)$.
3: Each node i sends $d_i(k) = x_i(k) - \beta_i(k)$ to node $\pi(i)$.
4: Each node i updates its state by

$$x_i(k+1) = \beta_i(k) + d_{\pi^{-1}(i)}(k).$$

5: Set $k \leftarrow k+1$ and go to step 1.

We term the described protocol as a Synchronous Iterative PPSP (SI-PPSP). The "synchronous" in SI–PPSP is in the sense that a global network clock is necessary, in order to schedule all nodes' communication and computation behaviors at each discrete time k. It is clear that the communication principle in Section II-B is met under SI-PPSP. We next show that the privacy and utility principles are also satisfied for the proposed protocol. On the one hand, at each time k, the only content that node i sends out is $d_i(k)$ to node $\pi(i)$, which contains not only its current state $x_i(k)$, but a random number $\beta_i(k)$ generated by itself, which prevents node $\pi(i)$ from perfectly learning about its true state. On the other hand, it can be shown by direct computation:

$$\begin{aligned} \sum_{i \in \mathrm{V}} x_i(k+1) &= \sum_{i \in \mathrm{V}} (\beta_i(k) + d_{\pi^{-1}(i)}(k)) \\ &= \sum_{i \in \mathrm{V}} \beta_i(k) + \sum_{i \in \mathrm{V}} (x_{\pi^{-1}(i)}(k) - \beta_{\pi^{-1}(i)}(k)) \\ &= \sum_{i \in \mathrm{V}} x_i(k). \end{aligned}$$

This implies that the network sum $\sum_{i \in \mathrm{V}} x_i(k)$ remains unchanged across the iteration process.

Evidently, a global clock is required within SI-PPSP, which involves a centralized perspective and slightly breaches the distributed setup. Based on [9], one can also provide an asynchronized version of SI-PPSP (called AI-PPSP) to facilitate distributed implementations, where each node is equipped with a local Poisson clock and the network demands no central scheduling.

Remark. *Relevant work is presented in [10], [11], where the information exchange rule that preserve network summation is used to shuffle node states, which turns out to be an universal privacy–preserving subroutine for distribution algorithms. In contrast, this paper proposes a sum evaluation protocol by introducing zero–mean random variables with diminishing variance.*

B. Comparisons with Existing Protocols

We now compare the proposed SI-PPSP with a few existing protocols to position it in a proper context and demonstrate its superiority. The goal of distributed average consensus protocols is similar to secure summation, in which nodes asymptotically achieve the network average as an agreement via local communications. The privacy-preserving versions of the consensus protocols, e.g., [6]–[8], provide a variety of approaches to computing the network average in a confidential fashion, which can be classified into two categories: statistical and cryptographical. In statistical methods, on the one hand, artificial noise is injected into original secrets [6] or node-to-node communication packets [7]. Neither statistical way guarantees fundamental convergence to the desired solution with the absence of a trusted third party. Moreover, their resilience against dynamic environments is left unexplored. On the other hand, cryptographical techniques leverage ciphers to protect information flows. Nevertheless, high computation and communication complexities are induced by the extremely frequent invocations of encryption, decryption and homomorphic operation schemes [8]. In the experimental section, we will further demonstrate the advantages of SI-PPSP in terms of accuracy, complexity and dynamic resilience.

It is well known that the secure sum protocol [2] solves the same problem in our paper by implementing finite-step orderly procedures over the same directed ring graph as in this paper. In the secure sum protocol, nevertheless, the secret of any node $i \in \mathrm{V}$ can be perfectly reconstructed under the collusion of only two nodes $\pi^{-1}(i), \pi(i)$. This is due to its unbalanced protocol structure, in which there is a master node and only this node generates a random variable passed down along the whole communication path. Indeed, the "secret share" method in [2] can increase the number of collusive nodes needed, but it also requires a varying network topology in return. In comparison, SI-PPSP, over an invariant ring graph which allows optimal communication resource allocation, guarantees that the privacy of each node's secret can never be inferred because of the random noise that keeps being created by each node at all times. In addition, it is difficult to deal with dynamic environments in the secure sum protocol, since the protocol terminates in finite steps and has to be completely re-executed once some node would like to join or leave after the termination. Even if the protocol is in the execution phase, the participating nodes who wants to leave must leave prior to the time when the information flow has not reached them. This significantly restricts the protocol's practicability and makes it incompatible with dynamic setup. In contrast, we will show that SI-PPSI allows nodes to join and leave at any time they want and has high applicability in dynamic scenarios.

IV. Main Results

A. Utility Analysis

Evidently, SI-PPSP is inherently not a consensus protocol and thus, node i cannot obtain the desired sum by directly observing an instantaneous state $x_i(k)$. The following theorem describes the way that a node retrieves the protocol output.

Theorem 1. *Consider sequences*

$$\{y_i(k)\}_{k=0}^{\infty} = \left\{ \sum_{r=0}^{n-1} x_i(k+r) \right\}_{k=0}^{\infty}$$

for all $i \in \mathrm{V}$. Then along SI-PPSP, the following statements hold for each $i \in \mathrm{V}$.

(i) If $v_i(k) = \frac{c_i}{k+d_i}$ with $c_i, d_i > 0$, then

$$\lim_{k\to\infty} \mathbb{E} \sum_{i\in\mathrm{V}} \left| y_i(k) - \sum_{j\in\mathrm{V}} s_j \right| \leq c_M \pi n \sqrt{\frac{n}{6}},$$

where $c_M = \max\{c_i : i \in \mathrm{V}\}$.

(ii) If $v_i(k) = c_i \phi_i^k$ with $c_i > 0$ and $0 < \phi_i < 1$, then

$$\lim_{k\to\infty} \mathbb{E} \sum_{i\in\mathrm{V}} \left| y_i(k) - \sum_{j\in\mathrm{V}} s_j \right| \leq \max_{i\in\mathrm{V}} c_i n \sqrt{\frac{n}{1-\phi_i^2}}.$$

The proof of Theorem 1 is provided in Appendix A. Evidently, $y_i(k)$ can be termed as a solution estimator. Theorem 1 clarifies that each node can add up n consecutive states of its own as an approximation of the network sum, after SI-PPSP executes for a sufficiently long time. Theorem 1 provides asymptotic upper bounds for the execution error of SI-PPSP in mean square expectation along time under two commonly used classes of random variance options. This clearly shed theoretic light on the utility of the proposed protocol.

B. Accuracy Analysis

In the following, we provide a lemma that assists with the proof of further results.

Lemma 1. *Consider matrices $\mathbf{C}^1, \ldots, \mathbf{C}^m \in \mathbb{R}^{n\times n}$ and random vectors $\mathbf{r}^1, \ldots, \mathbf{r}^m \in \mathbb{R}^n$. Suppose all the components of $\mathbf{r}^i$, $i = 1, \ldots, m$ are pairwise independent. Define $\sigma_{\mathrm{M}}^i = \max(\mathrm{diag}(\mathrm{cov}(\mathbf{r}^i)))$. Then*

$$\mathrm{tr}(\mathrm{cov}(\sum_{i=1}^{m} \mathbf{C}^i \mathbf{r}^i)) \leq \sum_{i=1}^{m} \|\mathbf{C}^i\|_{\mathrm{F}}^2 \sigma_{\mathrm{M}}^i.$$

The proof of Lemma 1 can be found in Appendix B. The following theorem studies the variance of the solution estimator.

Theorem 2. *Consider the same sequences $\{y_i(k)\}_{k=0}^{\infty}$, $i \in \mathrm{V}$ as in Theorem 1. Then along SI-PPSP, there holds $\lim_{k\to\infty} \mathbb{E}(y_i(k)) = \sum_{j\in\mathrm{V}} s_j$ for all $i \in \mathrm{V}$. Furthermore, for each $i \in \mathrm{V}$, the following conclusions can be drawn.*

(i) If $v_i(k) = \frac{c_i}{k+d_i}$ with $c_i, d_i > 0$, then

$$\lim_{k\to\infty} \sum_{i\in\mathrm{V}} \mathrm{var}(y_i(k)) \leq \frac{c_M^2 \pi^2 n^2}{3},$$

where $c_M = \max\{c_i : i \in \mathrm{V}\}$.

(ii) If $v_i(k) = c_i \phi_i^k$ with $c_i > 0$ and $0 < \phi_i < 1$, then

$$\lim_{k\to\infty} \sum_{i\in\mathrm{V}} \mathrm{var}(y_i(k)) \leq \max_{i\in\mathrm{V}} \frac{2n^2 c_i^2}{1-\phi_i^2}.$$

The proof of Theorem 2 can be found in Appendix C. Theorem 2 clarifies the convergence results for the variance of the solution estimator, providing measurement for the accuracy of SI-PPSP.

C. Privacy Analysis

Adversaries against a general privacy–preserving protocol can be simply classified as global and local ones. Global adversaries are usually powerful eavesdroppers, who have access to all communication contents shared among nodes and aim to recover all nodes' secrets based on these observations. In contrast, local adversaries are a subset of protocol participants, who obey the protocol rules but in the meantime try to infer the other nodes' secrets. Privacy analysis against local adversaries are usually termed as semi-honest security in the field of secure multiparty computation. In this section, we will focus on powerful global eavesdroppers for SI-PPSP, the privacy analysis against which will cover semi-honest assumptions.

In practical implementation, SI-PPSP is executed for finite time period $0, 1, \ldots, K-1$, which is called K–step SI-PPSP. Evidently, under SI-PPSP a global adversary aims to infer $\{s_i\}_{i\in \mathrm{V}}$ based on the observation $\{d_i(k)\}_{i\in \mathrm{V}, k=0,1,\ldots,K-1}$. Such a privacy reconstruction relation can be represented by a mapping $\mathcal{M}^K : \mathbb{R}^n \to \mathbb{R}^{nK}$, which maps the private data $\{s_i\}_{i\in \mathrm{V}}$ to the observation $\{d_i(k)\}_{i\in \mathrm{V}, k=0,1,\ldots,K-1}$. In the following, we formally introduce a few notions that assist with differential privacy analysis [12].

Definition 1. *Consider two network secrets* $\mathbf{s} = [s_1 \ \ldots \ s_n]^\top$ *and* $\mathbf{s}' = [s'_1 \ \ldots \ s'_n]^\top$ *in vector form. Then* $\mathbf{s}$ *and* $\mathbf{s}'$ *are said to be* δ*–adjacent if there exists a unique* $1 \le i \le n$ *such that* $s_j = s'_j$ *for all* $j \neq i$ *and*

$$|s_i - s'_i| \le \delta.$$

Definition 2. *SI-PPSP preserves* (ϵ, δ, K)*–differential privacy if*

$$\Pr(\mathcal{M}^K(\mathbf{s}) \subset \mathrm{R}) \le e^\epsilon \Pr(\mathcal{M}^K(\mathbf{s}') \subset \mathrm{R})$$

for all $\mathrm{R} \in \mathbb{R}^{nK}$ *and any two* δ*–adjacent secrets* $\mathbf{s}, \mathbf{s}' \in \mathbb{R}^n$.

For SI-PPSP, the following theorem holds.

Theorem 3. *Suppose* $\{\beta_i(k)\}_{i\in \mathrm{V}, k=0,1,\ldots,K-1}$ *are Laplace distributed random variables.*

(i) If $v_i(k) = \frac{c_i}{k+d_i}$ *with* $c_i, d_i > 0$*, then SI-PPSP preserves*

$$\left(c_m^{-1}\delta K\left(\frac{K-1}{2} + d_M\right), \delta, K\right)$$

–differential privacy, where $c_m = \min\{c_i : i \in \mathrm{V}\}$ *and* $d_M = \max\{d_i : i \in \mathrm{V}\}$.

(ii) If $v_i(k) = c_i\phi_i^k$ *with* $c_i > 0$ *and* $0 < \phi_i < 1$*, then SI-PPSP preserves*

$$\left(\frac{c_m^{-1}\delta(1-\phi_m^K)}{\phi_m^{K-1} - \phi_m^K}, \delta, K\right)$$

–differential privacy, where $c_m = \min\{c_i : i \in \mathrm{V}\}$ *and* $\phi_m = \min\{\phi_i : i \in \mathrm{V}\}$.

The proof of Theorem 3 can be found in Appendix D. Clearly, Theorem 3 guarantees that SI-PPSP can preserve differential privacy by only choosing the random noise $\beta_i(k)$ to be Laplace distributed, implying that it complys with state-of-the-art privacy metrics.

D. Utility, Accuracy and Privacy Tradeoff

The following definition is provided for specifying a class of adversaries.

Definition 3. *Adversaries who aim to distinguish* δ*–adjacent secrets* $\mathbf{s}, \mathbf{s}' \in \mathbb{R}^n$ *based on the observation* $\mathcal{M}^K(\mathbf{s})$ *and* $\mathcal{M}^K(\mathbf{s}')$ *are termed as* δ*–differential attackers.*

We now provide the following theorem to characterize the tradeoff among utility, accuracy and privacy–preserving capability of SI-PPSP.

Theorem 4. *Consider* K*–step SI-PPSP against* δ*–differential attackers. Let* $\gamma_u, \gamma_a, \gamma_p > 0$ *be fixed importance balancers for utility, accuracy and privacy. Let* $\mathscr{M}_u, \mathscr{M}_a, \mathscr{M}_p$ *denote the corresponding metrics concluded in Theorem 1, 2 and 3. Consider the tradeoff problem*

$$\min_{c_i>0, d_i\ge 0} \gamma_u \mathscr{M}_u + \gamma_a \mathscr{M}_a + \gamma_p \mathscr{M}_p.$$

Suppose $v_i(k) = \frac{c_i}{k+d_i}$ *with* $c_i > 0$ *and* $d_i \ge 0$*. Then necessarily and sufficiently the optimal* $d_1 = \cdots = d_n = 0$*, and the optimal choices of* c_i *are* $\bar{c} = c_1 = \cdots = c_n$ *being the real root of the following cubic equation*

$$4\gamma_a\pi^2 n^2 \bar{c}^3 + \sqrt{6}\gamma_u \pi n^{\frac{3}{2}} \bar{c}^2 - 3\gamma_p \delta K(K-1) = 0,$$

which always uniquely exists.

The proof of Theorem 4 can be found in Appendix E. For the $\frac{1}{k}$–decaying variance case, Theorem 4 provides guidance on appropriate selection of the decay parameters by taking into account the utility, accuracy and privacy–preserving capability. However, it is fairly difficult to provide theoretic analysis on the tradeoff problem for the exponentially decaying variance case, because it leads to a complex program and the solution is nontrivial.

E. Node Join and Leave

Common occasions may occur in which during the execution of PPSP a node chooses to drop out, or an external party would like to join the network sum evaluation. Such node is called a dynamic node. Note that privacy disclosure of the dynamic node's state to all nodes except for the neighbor of the dynamic node is trivial if they know its identity. Therefore, we assume that the dynamic node's identity is anonymous. It turns our that our SI-PPSP can perfectly support such disturbance with state update rule altered as follows.

Under SI-PPSP, if a node $i \in \mathrm{V}$ decides to leave at time k, it should send to $\pi(i)$

$$d_i(k) = x_i(k) - s_i,$$

inform $\pi^{-1}(i)$ of stopping sending out contents and altering update rule at time k as

$$x_{\pi^{-1}(i)}(k+1) = x_{\pi^{-1}(i)}(k) + d_{\pi^{-1}\circ\pi^{-1}(i)}(k),$$

and then leave. The whole network structure is updated by $\mathrm{G}^- = (\mathrm{V}^-, \mathrm{E}^-)$, where $\mathrm{V}^- = \mathrm{V} \setminus \{i\}$ and $\mathrm{E}^- = \mathrm{E} \bigcup \{(\pi^{-1}(i), \pi(i))\} \setminus \{(\pi^{-1}(i), i), (i, \pi(i))\}$. If an external party $i^+ \notin \mathrm{V}$ is to join, it selects a node $i^* \in \mathrm{V}$ and then directly updates the network by $\mathrm{G}^+ = (\mathrm{V}^+, \mathrm{E}^+)$, where $\mathrm{V}^+ = \mathrm{V} \bigcup \{i^+\}$ and $\mathrm{E}^+ = \mathrm{E} \bigcup \{(\pi^{-1}(i^*), i^+), (i^+, \pi(i^*))\} \setminus \{(\pi^{-1}(i^*), \pi(i^*))\}$, and the network G^+ can proceed to employ SI-PPSP.

V. Experiments

A. Simulation Setup

In this section, we consider the 100-node ring graph. All secrets $s_1, \ldots, s_{100}$ are independently and identically sampled from a normal distribution $\mathcal{N}(1, 1)$. In addition, we will arrange a node's joining and leaving during the execution, whose secret s_{101} is sampled from $\mathcal{N}(100, 1)$. Under this setup, we will verify the effectiveness of SI-PPSP in dynamic environments, and compare it with a few existing protocols in terms of accuracy, complexity and dynamic resilience. It is worth mentioning that the strategies against dynamic disturbance is unspecified but fairly straightforward for many existing works. Thus, we will adopt the similar method as SI-PPSP for them, i.e., direct joining with its state, and leaving after decomposing and sharing to the neighbors its initial state.

We implement all protocols on a computing machine with 40 CPU cores and 192GB RAM. In particular, we use the Paillier cryptosystem[1] as the encryption scheme to implement the homomorphic-encryption-based protocol [8].

B. Verification

We let SI-PPSP execute for 1500 rounds, during which time a node joins at $k = 500$ and leaves at $k = 1000$. We plot the trajectories of $y_i(k)$ for all $i \in \mathrm{V}$ in Figure 2. As shown in Figure 2, $y_i(k)$s asymptotically go to the desired sum. Besides, affected by the disturbance at $k = 500$ and $k = 1000$, node states are forced to deviate from the sum for a short period, but go back shortly. The effectiveness in computing secret sum and resilience against dynamic environments are clearly illustrated by Figure 2.

C. Evaluation

We now compare SI-PPSP with a few existing works [6]–[8]. Note that the artificial random noise introduced has variance of the same scale for SI-PPSP, [6], [7]. For these four protocols, we first collect the time consumed on their 1500-round execution in Table I. Table I demonstrates statistical methods, to which SI-PPSP belongs, has an overwhelming advantage over cryptographical methods in the terms of algorithm complexity. We then plot $\max_i |z_i(k) - s^*|$ in Figure 3, where $s^* = \sum_i s_i/n$, and $z_i(k) = y_i(k)/n$ for SI-PPSP

[1]https://github.com/data61/python-paillier

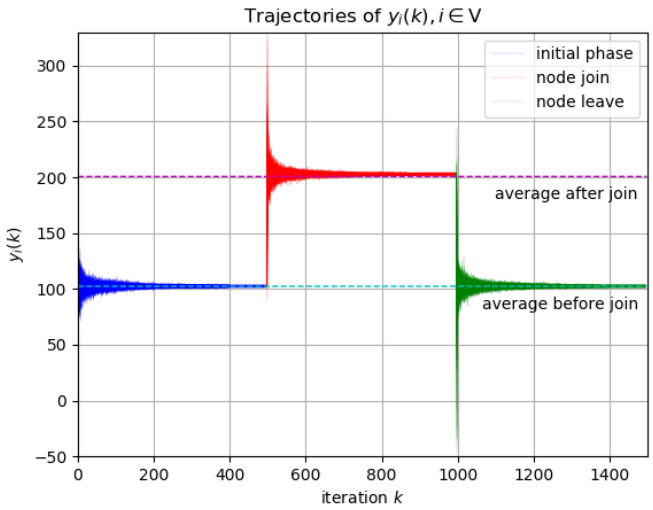


Fig. 2: Convergence along SI-PPSP

Protocol	SI-PPSP	Braca2016	He2017	Ruan2019
Execution Time (sec)	1.092	0.529	0.442	7.772×10^4

TABLE I: Complexity Comparison

and $z_i(k)$ is node i's state for the other protocols. Note that the second row of figures are a micro perspective of the first row. It can be seen from Figure 3 that it is difficult for $z_i(k)$'s trajectory to converge to the exact result for [6], [7]. In comparison, SI-PPSP drives $z_i(k)$ to exactly zero with the fastest convergence speed in the initial phase. Furthermore, after losing track of the average on a node's joining and leaving, it takes the least time to drive the network back on track for SI-PPSP. The superiority of SI-PPSP in terms of accuracy and dynamic resilience is now clearly illustrated.

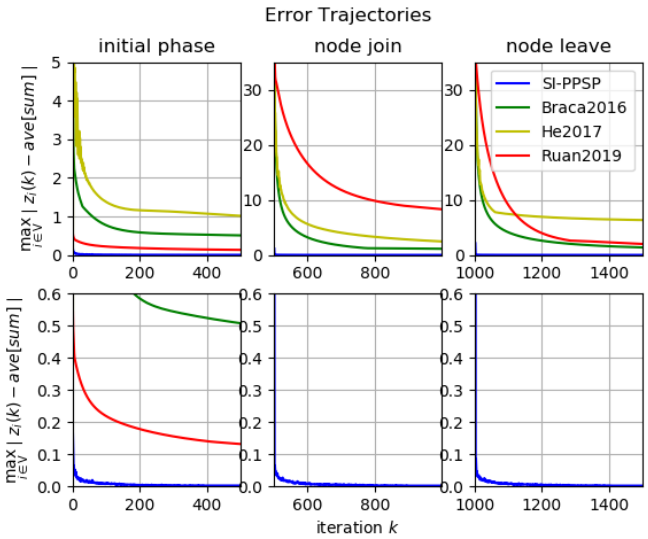


Fig. 3: Accuracy and Dynamic Resilience Comparison

VI. Conclusions

This paper studied the problem of evaluating the sum of network secrets. From the dynamic perspective, we proposed distributed privacy–preserving protocols for computing the sum, which are resilient against disturbance resulted from node join and leave. Theoretic convergence analysis was provided, demonstrated with several numerical examples that also verifies the effectiveness of the proposed protocols. We also showed that the proposed protocols preserve differential privacy and investigated the tradeoff problem among utility, accuracy and privacy, the solution to which enables us to provide guidance on appropriate selection of random noise parameters.

References

[1] R. Lu, X. Lin, Z. Shi, and X. Shen, "A lightweight conditional privacy-preservation protocol for vehicular traffic-monitoring systems," IEEE Intelligent Systems, vol. 28, pp. 62–65, 2013.

[2] C. Clifton, M. Kantarcioglu, J. Vaidya, X. Lin, and M. Y. Zhu, "Tools for privacy preserving distributed data mining," ACM Sigkdd Explorations Newsletter, vol. 4, pp. 28–34, 2002.

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

[4] I. Damgård, V. Pastro, N. Smart, S. Zakarias, "Multiparty computation from somewhat homomorphic encryption," Annual Cryptology Conference, pp. 643–662, 2012.

[5] Y. Mo, and R. M. Murray, "Privacy preserving average consensus," IEEE Transactions on Automatic Control, vol. 62, pp. 753–765, 2017.

[6] P. Braca, R. Lazzeretti, S. Marano, V. Matta, "Learning with privacy in consensus + obfuscation," IEEE Signal Processing Letters, vol. 23, no. 9, pp. 1174–1178, 2016.

[7] J. He, Jianping, L. Cai, C. Zhao, P. Cheng, X. Guan, "Privacy-preserving average consensus: privacy analysis and algorithm design," IEEE Transactions on Signal and Information Processing over Networks, vol. 5, no. 1, pp. 127–138, 2018.

[8] M. Ruan, H. Gao, Y. Wang, "Secure and privacy-preserving consensus," IEEE Transactions on Automatic Control, vol. 64, no. 10, pp. 4035–4049, 2019.

[9] S. Boyd, A. Ghosh, B. Prabhakar, and D. Shah, "Randomized gossip algorithms," IEEE/ACM Transactions on Networking, vol. 14, pp. 2508–2530, 2006.

[10] Y. Liu, J. Wu, R. M. Ian, and G. Shi, "Gossip algorithms that preserve privacy for distributed computation Part I: the algorithms and convergence conditions," IEEE Conference on Decision and Control, pp. 4499–4504, 2018.

[11] Y. Liu, J. Wu, R. M. Ian, and G. Shi, "Gossip algorithms that preserve privacy for distributed computation Part II: performance against eavesdroppers," IEEE Conference on Decision and Control, pp. 5346–5351, 2018.

[12] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," Theory of cryptography conference, pp. 265–284, 2006.

[13] P. J. Davis, "Circulant Matrices," American Mathematical Soc., 2013.

[14] F. D. Mcsherry, "Privacy integrated queries: an extensible platform for privacy-preserving data analysis," Proceedings of the 2009 ACM SIGMOD International Conference on Management of Data, pp. 19–30, 2009.

[15] S. Boyd, and L. Vandenberghe, "Convex Optimization," Cambridge university press, 2004.

Appendix

Appendix A. Proof of Theorem 1

Introduce

$$\mathbf{x}(k)=\begin{bmatrix}x_1(k)\\ \vdots\\ x_n(k)\end{bmatrix},\ \mathbf{y}(k)=\begin{bmatrix}y_1(k)\\ \vdots\\ y_n(k)\end{bmatrix},\ \boldsymbol{\beta}(k)=\begin{bmatrix}\beta_1(k)\\ \vdots\\ \beta_n(k)\end{bmatrix}.$$

We then rewrite node state dynamics of SI-PPSP compactly as

$$\mathbf{x}(k+1)=\mathbf{A}\mathbf{x}(k)+(\mathbf{I}_n-\mathbf{A})\boldsymbol{\beta}(k), \tag{1}$$

where $\mathbf{A}\in\mathbb{R}^{n\times n}$ is a circulant matrix in the form

$$\mathbf{A}=\begin{bmatrix}0 & 0 & \cdots & 0 & 1\\ 1 & 0 & \cdots & 0 & 0\\ 0 & 1 & \cdots & 0 & 0\\ \vdots & \vdots & \ddots & 0 & 0\\ 0 & 0 & \cdots & 1 & 0\end{bmatrix}.$$

Introduce $\mathbf{s}=[s_1\ \ldots\ s_n]^\top$ and $s=\mathbf{1}_n^\top\mathbf{s}$. Then it is immediate from (1)

$$\mathbf{x}(k)=\mathbf{A}^k\mathbf{s}+\sum_{m=0}^{k-1}\mathbf{A}^m(\mathbf{I}_n-\mathbf{A})\boldsymbol{\beta}(k-1-m). \tag{2}$$

We next study

$$\begin{aligned}
&\mathbb{E}\|\mathbf{y}(k)-s\mathbf{1}_n\|^2\\
&=\mathbb{E}\left\|\sum_{r=0}^{n-1}\mathbf{x}(k+r)-s\mathbf{1}_n\right\|^2\\
&\overset{\text{a)}}{=}\mathbb{E}\left\|\mathbf{A}^k\left(\sum_{r=0}^{n-1}\mathbf{A}^r\right)\mathbf{s}-s\mathbf{1}_n\right.\\
&\quad\left.+\sum_{l=k}^{k+n-1}\sum_{m=0}^{l-1}\mathbf{A}^m(\mathbf{I}_n-\mathbf{A})\boldsymbol{\beta}(l-1-m)\right\|^2\\
&\overset{\text{b)}}{=}\left\|\mathbf{A}^k\left(\sum_{r=0}^{n-1}\mathbf{A}^r\right)\mathbf{s}-s\mathbf{1}_n\right\|^2\\
&\quad+\mathbb{E}\left\|\sum_{l=k}^{k+n-1}\sum_{m=0}^{l-1}\mathbf{A}^m(\mathbf{I}_n-\mathbf{A})\boldsymbol{\beta}(l-1-m)\right\|^2,
\end{aligned} \tag{3}$$

where a) follows (2), and b) is obtained by omitting those terms containing $\mathbb{E}\beta(k)$ due to the zero mean assumption on $\beta_i(k)$s. We now analyze the first term in (3). According to [13], $\mathbf{A}$ is diagonalizable as $\mathbf{A}=\mathbf{Q}\boldsymbol{\Lambda}\mathbf{Q}^\top$, where the i–th column of $\mathbf{Q}\in\mathbb{R}^{n\times n}$ is given by

$$\begin{aligned}
\mathbf{q}_i&=\frac{1}{\sqrt{n}}\begin{bmatrix}1 & w_i & w_i^2 & \ldots & w_i^{n-1}\end{bmatrix}^\top,\\
w_i&=\exp\left(j\frac{2\pi(i-1)}{n}\right),
\end{aligned}$$

and $\mathbf{\Lambda} = \mathrm{diag}(w_1^{n-1}, \ldots, w_n^{n-1})$ is a diagonal matrix. Then

$$\begin{aligned}\sum_{r=0}^{n-1} \mathbf{A}^r &= \mathbf{Q} \sum_{r=0}^{n-1} \mathbf{\Lambda}^r \mathbf{Q}^\top \\ &= \mathbf{Q} \begin{bmatrix} \sum\limits_{r=0}^{n-1} w_1^{r(n-1)} & & \\ & \ddots & \\ & & \sum\limits_{r=0}^{n-1} w_n^{r(n-1)} \end{bmatrix} \mathbf{Q}^\top. \end{aligned} \tag{4}$$

For $i = 2, \ldots, n$, direct computation shows if n is even

$$w_i^{r(n-1)} = \begin{cases} w_i^{(n-r)(n-1)} & \text{if } r \neq 0; \\ 1 & \text{otherwise,} \end{cases}$$

and if n is odd, then it is satisfied

$$\begin{aligned}\sum_{r=1}^{(n-1)/2} \mathrm{Re}(w_i^{r(n-1)}) = \sum_{(n+1)/2}^{n-1} \mathrm{Re}(w_i^{r(n-1)}) = -\frac{1}{2}, \\ \mathrm{Im}(w_i^{r(n-1)}) = \mathrm{Im}(w_i^{(n-r)(n-1)}).\end{aligned}$$

Hence, (4) yields $\sum\limits_{r=0}^{n-1} \mathbf{A}^r = n\mathbf{q}_1\mathbf{q}_1^\top$, based on which one has

$$\begin{aligned}&\lim_{k=\infty} \left\| \mathbf{A}^k \left(\sum_{r=0}^{n-1} \mathbf{A}^r \right) \mathbf{s} - s\mathbf{1}_n \right\|^2 \\ &= \lim_{k=\infty} \left\| \begin{bmatrix} \mathbf{q}_1 & \cdots & \mathbf{q}_n \end{bmatrix} \begin{bmatrix} w_1^{k(n-1)} & & \\ & \ddots & \\ & & w_n^{k(n-1)} \end{bmatrix} \right. \\ &\quad \left. \cdot \begin{bmatrix} n\mathbf{q}_1^\top \\ 0 \\ \vdots \\ 0 \end{bmatrix} \mathbf{s} - s\mathbf{1}_n \right\|^2 \\ &= n^2 \|\mathbf{q}_1\mathbf{q}_1^\top\|^2 + s^2\|\mathbf{1}_n\|^2 - 2ns\mathbf{q}_1^\top \mathbf{1}_n \mathbf{q}_1^\top \mathbf{s} \\ &= 0. \end{aligned} \tag{5}$$

We next investigate the second term in (3):

$$\begin{aligned}&\lim_{k\to\infty} \mathbb{E} \left\| \sum_{l=k}^{k+n-1} \sum_{m=0}^{l-1} \mathbf{A}^m (\mathbf{I}_n - \mathbf{A}) \boldsymbol{\beta}(l-1-m) \right\|^2 \\ &\overset{\text{a)}}{\leq} \lim_{k\to\infty} \sum_{l=k}^{k+n-1} \sum_{m=0}^{l-1} \mathbb{E} \left\| \mathbf{A}^m (\mathbf{I}_n - \mathbf{A}) \boldsymbol{\beta}(l-1-m) \right\|^2 \\ &\overset{\text{b)}}{\leq} \lim_{k\to\infty} \sum_{l=k}^{k+n-1} \sum_{m=0}^{l-1} \mathbb{E} \|\boldsymbol{\beta}(l-1-m)\|^2 \\ &= \lim_{k\to\infty} \sum_{l=k}^{k+n-1} \sum_{m=0}^{l-1} \sum_{i\in\mathrm{V}} v_i^2(l-1-m) \\ &\leq n^2 \max_{i\in\mathrm{V}} \sum_{k=0}^{\infty} v_i^2(k) \\ &\overset{\text{c)}}{\leq} \begin{cases} \dfrac{c_M^2 \pi^2 n^2}{6} & \text{if } v_i(k) = \dfrac{c_i}{k+d_i}; \\ n^2 \max\limits_{i\in\mathrm{V}} \dfrac{c_i^2}{1-\phi_i^2} & \text{if } v_i(k) = c_i \phi_i^k, \end{cases} \end{aligned} \tag{6}$$

where a) and b) come from norm inequalities and c) is from simple calculation of infinite series. Then the proof of the desired statements is completed by (5), (5) and the Cauchy-Schwarz inequality

$$\begin{aligned}\sum_{i\in\mathrm{V}} \left| y_i(k) - \sum_{j\in\mathrm{V}} s_j \right| &\leq \sqrt{\sum_{i\in\mathrm{V}} \left| y_i(k) - \sum_{j\in\mathrm{V}} s_j \right|^2} \cdot \sqrt{\sum_{i\in\mathrm{V}} 1^2} \\ &= \sqrt{n} \|\mathbf{y}(k) - s\mathbf{1}\|.\end{aligned}$$

Appendix B. Proof of Lemma 1

Let c_{jl}^i denote the jl–th entry of $\mathbf{C}^i$, and r_l^i denote the l–th component of $\mathbf{r}^i$. Based on the pairwise independence assumption, one can directly write

$$\begin{aligned}&\mathrm{tr}(\mathrm{cov}(\sum_{i=1}^{m} \mathbf{C}^i \mathbf{r}^i)) \\ &= \mathrm{tr}(\mathrm{cov} \begin{bmatrix} \sum\limits_{i=1}^{m} \sum\limits_{l=1}^{n} c_{1l}^i r_l^i \\ \vdots \\ \sum\limits_{i=1}^{m} \sum\limits_{l=1}^{n} c_{nl}^i r_l^i \end{bmatrix}) \\ &= \sum_{j=1}^{n} \mathrm{var}(\sum_{i=1}^{m} \sum_{l=1}^{n} c_{jl}^i r_l^i) \leq \sum_{i=1}^{m} \sum_{j=1}^{n} \sum_{l=1}^{n} (c_{jl}^i)^2 \,\mathrm{var}(r_l^i) \\ &\leq \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \sum_{l=1}^{n} (c_{jl}^i)^2 \right) \sigma_{\mathrm{M}}^i = \sum_{i=1}^{m} \|\mathbf{C}^i\|_{\mathrm{F}}^2 \sigma_{\mathrm{M}}^i,\end{aligned}$$

which completes the proof.

APPENDIX C. PROOF OF THEOREM 2

We will continue to use the notations $\mathbf{y}(k), \boldsymbol{\beta}(k), \mathbf{A}, \mathbf{Q}, \mathbf{\Lambda}, w_1, \ldots, w_n$ in the proof of Theorem 1. Then it follows (2) and the analysis in (5)

$$\mathbb{E}\mathbf{y}(k) = \mathbf{A}^k \left(\sum_{r=0}^{n-1} \mathbf{A}^r \right) \mathbf{s} = s\mathbf{1}.$$

Define $\sigma_{\mathrm{M}}(k) = \max(\mathrm{diag}(\mathrm{cov}(\boldsymbol{\beta}(k))))$. Again based on (2), one has using Lemma 1

$$\begin{aligned}
&\sum_{i\in\mathrm{V}} \mathrm{var}(y_i(k)) = \mathrm{tr}(\mathrm{cov}(\mathbf{y}(k))) \\
&= \mathrm{tr}(\mathrm{cov}(\sum_{l=k}^{k+n-1} \sum_{m=0}^{l-1} \mathbf{A}^m(\mathbf{I}_n - \mathbf{A})\boldsymbol{\beta}(l-1-m)) \\
&\leq \sum_{l=k}^{k+n-1} \sum_{m=0}^{l-1} \|\mathbf{A}^m(\mathbf{I}_n - \mathbf{A})\|_{\mathrm{F}}^2 \sigma_{\mathrm{M}}(l-1-m) \\
&\leq \sum_{l=k}^{k+n-1} \sum_{m=0}^{l-1} \|\mathbf{A}\|_{\mathrm{F}}^{2m} \|\mathbf{I}_n - \mathbf{A}\|_{\mathrm{F}}^2 \sigma_{\mathrm{M}}(l-1-m) \\
&= 2n \sum_{l=k}^{k+n-1} \sum_{m=0}^{l-1} \sigma_{\mathrm{M}}(l-1-m). \qquad (7)
\end{aligned}$$

Let k go to infinity in (7). Then one can easily obtain the desired result with simple series computation.

APPENDIX D. PROOF OF THEOREM 3

We will continue to use the following notations in the Appendix A: $\mathbf{x}(k), \boldsymbol{\beta}(k), \mathbf{s}$. Additionally, the superscript symbol prime on a vector $\mathbf{v}'$ is assumed to apply to each of its components. It is fairly hard to directly study the overall mapping $\mathcal{M}$. Instead, one can iteratively define a time–varying mapping $\mathcal{M}_k(\mathbf{x}(k)) = \mathbf{d}(k)$ with $\mathbf{d}(k) = [d_1(k) \ \ldots \ d_n(k)]^\top$. Evidently, there holds

$$\mathcal{M}^K = \{\mathcal{M}_k \circ \cdots \circ \mathcal{M}_0(\mathbf{s})\}_{k=1,\ldots,K-1} \bigcup \mathcal{M}_0(\mathbf{s}).$$

Assuming that each $\mathcal{M}_k$ preserves $(\epsilon_k, \delta, 1)$–differential privacy, according to [14], $\mathcal{M}^K$ preserves $\max\left\{ \sum_{k=0}^{l} \epsilon_k : l = 0, 1, \ldots, K-1 \right\}$, namely $\sum_{k=0}^{K-1} \epsilon_k$–differential privacy. The rest of the proof will clarify the way of calculating ϵ_k. For two δ–adjacent secrets $\mathbf{x}(k), \mathbf{x}'(k) \in \mathbb{R}$ differing at the i^*–th component, there holds

$$\begin{aligned}
&\frac{\Pr(\mathcal{M}_k(\mathbf{x}(k)) \subset \mathrm{R})}{\Pr(\mathcal{M}_k(\mathbf{x}'(k)) \subset \mathrm{R})} \\
&\overset{\text{a)}}{=} \frac{f_{\boldsymbol{\beta}}(\mathbf{x}(k) - \mathbf{d}(k))}{f_{\boldsymbol{\beta}}(\mathbf{x}'(k) - \mathbf{d}(k))} \\
&\overset{\text{b)}}{=} \exp\left(\sum_{i=1}^{n} \frac{|x_i'(k)| - |x_i(k)|}{v_i(k)} \right) \\
&\leq \exp\left(\frac{|x_{i^*}'(k) - x_{i^*}(k)|}{v_{i^*}(k)} \right) \\
&= \exp\left(\delta v_{i^*}^{-1}(k)\right), \qquad (8)
\end{aligned}$$

where a) is by the definition of probability and b) comes from the fact that $\boldsymbol{\beta}$ is Laplace distributed. We next discuss (8) in two cases.

(i) If $v_i(k) = \frac{c_i}{k+d_i}$, then there holds

$$v_i(k) \geq \frac{c_m}{k + d_M}. \qquad (9)$$

Then it follows (8) and (9)

$$\frac{\Pr(\mathcal{M}_k(\mathbf{x}(k)) \subset \mathrm{R})}{\Pr(\mathcal{M}_k(\mathbf{x}'(k)) \subset \mathrm{R})} \leq \exp\left(c_m^{-1}\delta(k + d_M)\right). \qquad (10)$$

From (10), one has $\epsilon_k = c_m^{-1}\delta(k + d_M)$, which leads to

$$\epsilon = \sum_{k=0}^{K-1} \epsilon_k = c_m^{-1}\delta K(\frac{K-1}{2} + d_M),$$

which completes the proof of (i).

(ii) If $v_i(k) = c_i\phi_i^k$, it is analogous $v_i(k) \geq c_m\phi_m^k$. Then

$$\epsilon_k = c_m^{-1}\delta\phi_m^{-k}$$

and

$$\epsilon = \sum_{k=0}^{K-1} \epsilon_k = \frac{c_m^{-1}\delta(1 - \phi_m^K)}{\phi_m^{K-1} - \phi_m^K}.$$

This completes the proof of (ii).

APPENDIX E. PROOF OF THEOREM 4

(i) Suppose $v_i(k) = \frac{c_i}{k+d_i}$. According to Theorem 1, 2 and 3, one can summarize the tradeoff among utility, accuracy and privacy as the following optimization problem:

$$\begin{aligned}
\min_{c_M, c_m > 0, d_M \geq 0} \quad & \gamma_u c_M \pi n \sqrt{\frac{n}{6}} + \gamma_a \frac{c_M^2 \pi^2 n^2}{3} \\
& + \gamma_p \left(c_m^{-1}\delta K \left(\frac{K-1}{2} + d_M \right) \right) \qquad (11) \\
\text{s.t.} \quad & c_M \geq c_m.
\end{aligned}$$

Since the term of d_M in the objective of (11) is linear and its coefficient $\gamma_p c_m^{-1}\delta K$ is strictly positive, the optimal d_M should be zero independently. Then the optimization problem (11) can be compactly written as $U(\boldsymbol{\theta})$

$$\begin{aligned}
\min_{\boldsymbol{\theta}\in\Theta} \quad & U(\boldsymbol{\theta}) \\
\text{s.t.} \quad & \mathbf{p}^\top\boldsymbol{\theta} \leq 0
\end{aligned} \qquad (12)$$

where

$$\begin{aligned}
\mathbf{p} &= \begin{bmatrix} -1 & 1 \end{bmatrix}^\top, \\
\Theta &= \left\{ \begin{bmatrix} \theta_1 & \theta_2 \end{bmatrix}^\top \in \mathbb{R}^2 : \theta_1, \theta_2 > 0 \right\}, \\
U(\boldsymbol{\theta}) &= \gamma_u \theta_1 \pi n \sqrt{\frac{n}{6}} + \gamma_a \frac{\theta_1^2 \pi^2 n^2}{3} \\
&\quad + \gamma_p \theta_2^{-1} \delta K \left(\frac{K-1}{2} \right).
\end{aligned}$$

Note that the variables θ_1 and θ_2 in (12) represents c_M and c_m, respectively. It can be easily shown that (12) is a convex optimization problem because Θ is a convex set, and the objective U and the constraint are both convex functions of $\boldsymbol{\theta}$.

Since the constraint $\mathbf{p}^\top \boldsymbol{\theta}$ is an affine function, weak Slater's condition and thus strong duality holds for (12) according to Section 5.2.3 in [15]. Therefore, $\boldsymbol{\theta}^* \in \mathbb{R}^2$ is optimal for (12) if and only if the following Karush–Kuhn–Tucker conditions hold:

$$\nabla U(\boldsymbol{\theta}^*) = -\mu \mathbf{p}, \tag{13}$$

$$\mu \mathbf{p}^\top \boldsymbol{\theta} = 0 \tag{14}$$

for some $\mu \geq 0$. Direct computation shows

$$\nabla U(\boldsymbol{\theta}) = \begin{bmatrix} \frac{2\gamma_a \pi^2 n^2}{3}\theta_1 + \gamma_u \pi n \sqrt{\frac{n}{6}} \\ -\frac{\gamma_p \delta K(K-1)}{2\theta_2^2} \end{bmatrix}. \tag{15}$$

Next we study the equation set (13)–(15). It is evident from (15) $\nabla U(\boldsymbol{\theta}^*) \neq 0$, and thus by (13) $\mu \neq 0$. As a result of (14), there must hold

$$\theta_1 = \theta_2. \tag{16}$$

In addition, by (13) and (15), one has

$$\frac{2\gamma_a \pi^2 n^2}{3}\theta_1 + \gamma_u \pi n \sqrt{\frac{n}{6}} = \frac{\gamma_p \delta K(K-1)}{2\theta_2^2}. \tag{17}$$

The equation set (16)–(17) finally leads to a cubic function with respect to θ:

$$g(\theta) = 4\gamma_a \pi^2 n^2 \theta^3 + \sqrt{6}\gamma_u \pi n^{\frac{3}{2}} \theta^2 - 3\gamma_p \delta K(K-1) = 0. \tag{18}$$

Since $g(0) < 0$ and there exists $\hat{\theta} > 0$ such that $g(\theta) \geq g(\hat{\theta}) \geq 0$ for all $\theta \geq \hat{\theta}$, it can be concluded that there at least exists one $0 < \theta^* < \hat{\theta}$ such that $g(\theta^*) = 0$, i.e., θ^* is a positive real root of (18). Next we show such θ^* is unique. One can directly compute

$$g'(\theta) = 12\gamma_a \pi^2 n^2 \theta^2 + 2\sqrt{6}\gamma_u \pi n^{\frac{3}{2}} \theta.$$

It can be seen that $g'(\theta) > 0$ for all $\theta > 0$, implying that $g(\theta)$ is strictly increasing over $(0, \infty)$. This results in the uniqueness of θ^* and completes the proof of (i).

(ii) We now consider the $v_i(k) = c_i \phi_i^k$ case and continue to use the notations c_M, c_m, ϕ_M, ϕ_m to represent the maximum or minimum of all c_is and ϕ_is. To simplify the tradeoff analysis, we slightly loosen the results of Theorem 1 and 2 to

$$\lim_{k\to\infty} \mathbb{E} \sum_{i\in \mathrm{V}} \left| y_i(k) - \sum_{j\in \mathrm{V}} s_j \right| \leq c_M n \sqrt{\frac{n}{1-\phi_M^2}}, \tag{19}$$

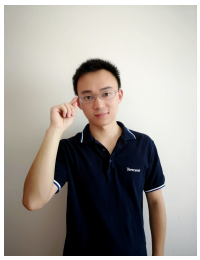
$$\lim_{k\to\infty} \sum_{i\in \mathrm{V}} \mathrm{var}(y_i(k)) \leq \frac{2n^2 c_M^2}{1-\phi_M^2}. \tag{20}$$

Based on (19), (20) and Theorem 3, one can express the tradeoff problem as

$$\begin{aligned} \min_{c_M, c_m > 0, 0 < \phi_m, \phi_M < 1} \quad & \gamma_u c_M n \sqrt{\frac{n}{1-\phi_M^2}} + \gamma_a \frac{2n^2 c_M^2}{1-\phi_M^2} \\ & + \gamma_u \frac{c_m^{-1} \delta (1-\phi_m^K)}{\phi_m^{K-1} - \phi_m^K} \\ \text{s.t.} \quad & c_M \geq c_m. \end{aligned} \tag{21}$$

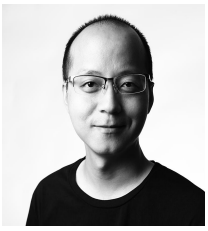
Yang Liu received the B.Eng. degree from the Department of Microelectronics, Tsinghua University, Beijing, China in 2015. Since Dec. 2015, he has been a Ph.D student at the Research School of Engineering, The Australian National University, Canberra, Australia. He is currently a senior researcher at Tencent, Shenzhen, China. His research interests include federated learning, secure multiparty computation, privacy preservation and acceleration for distributed computing.

Qingchen Liu received his Ph.D degree in system and control from Australian National University, Canberra, Australia, in 2018. He is currently an EuroTec Research Fellow within the Chair of Information-Oriented Control, Technical University of Munich, Munich, Germany. His research interest includes networked systems, distributed computation and multi-agent systems.



Xiong Zhang received the M.Eng. degree from School of Computer Science and Technology, Huazhong University of Science & Technology, Wuhan, China. Since 2017, he has been a senior engineer at Tencent, Shenzhen, China. His research interests include batch processing systems, distributed systems and big data.

Shuqi Qin received the M.Eng. degree from School of Information and Communication Engineering, Beijing University of Posts and Telecommunications , Beijing, China. She has been a senior big data engineer with over five years of experience in building data intensive applications, tackling challenging architectural and scalability problems in multiple scenarios.



Xiaoping Lei received the M.Eng. degree from School of Computer Science and Technology, Huazhong University of Science & Technology, Wuhan, China. He is currently an associate director at Tencent, Shenzhen, China. His research interests include batch processing systems, distributed systems and big data.