

Article

Adaptive Privacy-Preserving Coded Computing with Hierarchical Task Partitioning

Qicheng Zeng , Zhaojun Nan * and Sheng Zhou

Department of Electronic Engineering, Tsinghua University, Beijing 100084, China; zengqc19@mails.tsinghua.edu.cn (Q.Z.); sheng.zhou@tsinghua.edu.cn (S.Z.)

* Correspondence: nzj660624@mail.tsinghua.edu.cn

Abstract: Coded computing is recognized as a promising solution to address the privacy leakage problem and the straggling effect in distributed computing. This technique leverages coding theory to recover computation tasks using results from a subset of workers. In this paper, we propose the adaptive privacy-preserving coded computing (APCC) strategy, designed to be applicable to various types of computation tasks, including polynomial and non-polynomial functions, and to adaptively provide accurate or approximated results. We prove the optimality of APCC in terms of encoding rate, defined as the ratio between the computation loads of tasks before and after encoding, based on the optimal recovery threshold of Lagrange Coded Computing. We demonstrate that APCC guarantees information-theoretical data privacy preservation. Mitigation of the straggling effect in APCC is achieved through hierarchical task partitioning and task cancellation, which further reduces computation delays by enabling straggling workers to return partial results of assigned tasks, compared to conventional coded computing strategies. The hierarchical task partitioning problems are formulated as mixed-integer nonlinear programming (MINLP) problems with the objective of minimizing task completion delay. We propose a low-complexity maximum value descent (MVD) algorithm to optimally solve these problems. The simulation results show that APCC can reduce the task completion delay by a range of 20.3% to 47.5% when compared to other state-of-the-art benchmarks.

Keywords: coded computing; privacy preservation; hierarchical task partitioning; task cancellation; MINLP



Citation: Zeng, Q.; Nan, Z.; Zhou, S. Adaptive Privacy-Preserving Coded Computing with Hierarchical Task Partitioning. *Entropy* **2024**, *26*, 881. <https://doi.org/10.3390/e26100881>

Academic Editor: T. Aaron Gulliver

Received: 25 August 2024

Revised: 11 October 2024

Accepted: 15 October 2024

Published: 21 October 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Under the vision of “Internet of Everything”, intelligence-enabled applications are essential, leading to a variety of crucial computation tasks, such as the training and inference of complex machine learning models based on extensive datasets [1–3]. However, executing these computation-intensive tasks on a single device with limited computation capability and power resources presents significant challenges. To this end, distributed computing emerges as a practical solution, where a central node, referred to as *master*, manages task division, assignment, and result collection, while multiple distributed computing nodes, called *workers*, process the assigned partial computation tasks in parallel [4].

Nevertheless, while distributed computing accelerates the computation process by employing multiple workers for parallel processing, the total delay is dominated by the slowest worker, as the master must wait for all workers to complete their assigned tasks [5]. As demonstrated in the experimental results of [6], the delay of the slowest worker can exceed five times that of the others, which significantly prolongs the total delay. Moreover, due to the randomness of delays, identifying slow workers in advance is challenging. To tackle this so-called *straggling effect*, coded computing has emerged as a promising solution [6–12]. As Figure 1 shows, this approach combines coding theory with distributed computing and reduces delays by introducing structured computational redundancies.

Through the incorporation of redundancy during the encoding process, computation tasks can be completed using results from a subset of workers, thereby reducing total delays.

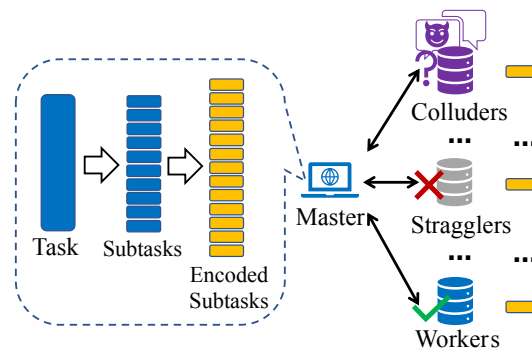


Figure 1. The concept of coded computing.

In coded computing, workers are tasked with processing input data and returning results, but the involved tasks may contain sensitive information, such as patient medical data, customer personal information, and proprietary company data [13,14]. Consequently, it is essential to maintain the data *privacy* against colluding workers, those who return correct results but may communicate with one another to share input data from the master, so as to infer some private information of the master. Recent research studies have aimed to develop coded computing strategies that address not only the straggling effect but also privacy concerns, such as combining additional random data insertion with prevalent polynomial coded computing methods [15–25]. This approach enhances the robustness of the system against straggling workers while also improving privacy and security by obscuring the original data.

In the majority of existing studies, matrix multiplication is treated as the primary application of coded computing, and its performance has been extensively validated. However, real-world computation tasks are often more diverse than mere matrix multiplication. For instance, in a linear regression task, the iterative process of solving weights involves calculating previous weights multiplied by the quadratic power of the input data. This implies that coded computing schemes for matrix multiplication must be executed twice in each step, and computation becomes considerably more complex when considering other tasks, such as inference tasks of neural networks.

In terms of extending the applicability of coded computing, one state-of-the-art approach is Lagrange Coded Computing (LCC) [15]. LCC employs Lagrange polynomial interpolation to transform input data before and after encoding into interpolation points on the computation function. This allows the recovery of desired results through the reconstruction of the interpolation function. LCC is compatible with various computation tasks, ranging from matrix multiplication to polynomial functions, and offers an optimal recovery threshold concerning the degree of polynomial functions. In [21,25,26], the problem of using matrix data as input and polynomial functions as computation tasks is also explored.

However, LCC still suffers from several shortcomings [27]. First, its recovery threshold is proportional to degrees of polynomial functions, which can be prohibitively large for complex tasks and thereby make it difficult to achieve successful recovery. Second, Lagrange polynomial interpolation can be ill-conditioned, making it challenging to ensure numerical stability, unless one embeds the computation to a finite field. In [27], Berrut's Approximated Coded Computing (BACC) is proposed to address these shortcomings and further expand the scope of computation tasks to arbitrary functions. However, BACC only yields approximated computing results and does not guarantee privacy preservation. Other related works [28–32] also focus on approximated results while attempting to maintain the numerical stability of coded computing. As far as we know, there is still a lack of a versatile coded computing strategy suitable for various computational tasks. This strategy should

be capable of achieving privacy preservation while providing accurate or approximated results based on specific demands.

On the other hand, opportunities exist to enhance mitigation of the straggling effect and further reduce delays. This is because prior studies commonly discard results from straggling workers, leading to the inefficient utilization of computational resources. In [11], a hierarchical task partitioning structure is proposed, where divided tasks are further partitioned into multiple layers, and workers process their assigned tasks in the order of layer indices. Consequently, straggling workers can return results from lower layers instead of none, while fast workers can reach higher layers and return more results. Similar performance improvements are achieved through multi-message communications (MMC) [33–35], where workers are permitted to return partial results of assigned tasks in each time slot, enabling straggling workers to contribute to the system.

Essentially, three ways exist to alleviate the straggling effect, given the total number of workers. First, minimize the recovery threshold of coded computing schemes, as a smaller recovery threshold implies fewer workers to wait for [9,10,15,16,36–39]. As a result, the master can recover desired computing results even with more straggling workers. Second, the computation loads for each worker should be carefully designed to allow them to complete varying amounts of computation based on their capabilities, which is formulated as optimization problems in [4,40–43]. This approach narrows the gap between the delays of fast and slow workers. Third, workers should be capable of returning partial results of assigned tasks, rather than the scenario where fast workers complete all assigned tasks, leaving straggling workers to contribute virtually nothing. The third point aligns with the idea of a hierarchical task partitioning structure and MMC.

In this work, we consider a distributed system with one master and multiple workers, and propose an adaptive privacy-preserving coded computing (APCC) strategy. The strategy primarily focuses on the applicability for diverse computation tasks, the privacy preservation of input data, and the mitigation of the straggling effect. Moreover, based on the hierarchical task partitioning structure in APCC, we propose an operation called *cancellation* to prevent slower workers from processing completed tasks, reducing resource waste and improving delay performance. Specifically, the main contributions are summarized as follows:

- We propose the APCC framework, which effectively mitigates the straggling effect and fully preserves data privacy. APCC is applicable to various computation tasks, including polynomial and non-polynomial functions, and can adaptively provide accurate results or approximated results with controllable error.
- We rigorously prove the information-theoretical privacy preservation of the input data in APCC, as well as the optimality of APCC in terms of the encoding rate based on the optimal recovery threshold of LCC. The encoding rate is defined as the ratio between the computation loads of tasks before and after encoding, serving as an indicator of the performance of coded computing schemes in mitigating the straggling effect.
- Considering the randomness of task completion delay, we formulate hierarchical task partitioning problems in APCC, with or without cancellation, as mixed-integer nonlinear programming (MINLP) problems with the objective of minimizing task completion delay. We propose a maximum value descent (MVD) algorithm to optimally solve the problems with linear complexity.
- Extensive simulations demonstrate improvements in delay performance offered by APCC when compared to other state-of-the-art coded computing benchmarks. Notably, APCC achieves a reduction in task completion delay ranging from 20.3% to 47.5% compared to LCC [15] and BACC [27]. Simulations also explore the trade-off between task completion delay and the level of privacy preservation.

The remainder of the paper is structured as follows. Section 2 presents the system model. In Section 3, we propose the adaptive privacy-preserving coded computing strategy, namely APCC. In Section 4, the performance of APCC is further analyzed in terms of encoding rate, privacy preservation, approximation error, numerical stability, communication

costs, and encoding and decoding complexity. In Section 5, we proposed the MVD algorithm to address the hierarchical task partitioning optimization problem with or without cancellation. The simulation results are provided in Section 6, and conclusions are drawn in Section 7.

2. System Model

As shown in Figure 2, we consider the distributed computing system consisting of one master and N workers. The goal is to complete a computation task on the master with the help of N workers. The task is represented by a function f , operating over an equally pre-divided input dataset $\mathbf{D} = \{\mathbf{D}_k \in \mathbb{R}^{p \times q} | k \in [0 : K - 1]\}$. The master aims to evaluate the results $\{f(\mathbf{D}_k)\}_{k=0}^{K-1}$, whose dimensions are decided by the task function f . To achieve this, we employ the proposed APCC strategy. Note that we consider the computation of $\{f(\mathbf{D}_k)\}_{k=0}^{K-1}$ as the entire task and the computation of $f(\mathbf{D}_k)$ as a subtask.

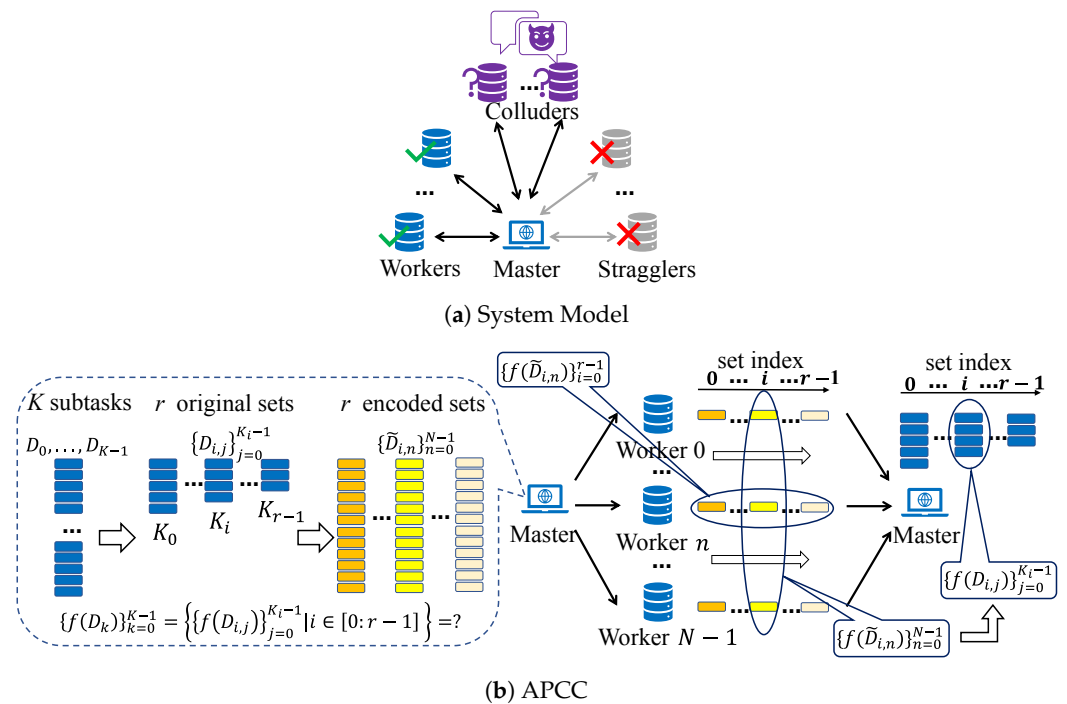


Figure 2. System model and the proposed Adaptive Privacy-preserving Coded Computing (APCC).

In APCC, the K equally pre-divided input data $\{\mathbf{D}_k\}_{k=0}^{K-1}$ are not directly encoded like conventional coded computing strategies. Instead, they are firstly partitioned into r sets. Subsequently, the input data in each set are encoded into N parts, which are then assigned to N workers for parallel computation. This hierarchical task partitioning structure enables workers to return partial results of assigned subtasks, further mitigating the straggling effect and reducing delays. After the task assignment, the master leverages the results obtained from a subset of workers in each set and employs interpolation methods to reconstruct the original function f , thereby achieving the recovery of $\{f(\mathbf{D}_k)\}_{k=0}^{K-1}$. A comprehensive description of the APCC strategy is presented in Section 3.

Taking into account the unreliable channels and uncertain computation capabilities of workers, some of them may fail to return results to the master in time. These straggling workers are referred to as *stragglers*. Additionally, we assume that workers are honest but curious. This means they will send back the correct computation results, but there could be up to L ($L < N$) colluding workers who can communicate with each other and attempt to learn information about the input data $\{\mathbf{D}_k\}_{k=0}^{K-1}$. These workers are called *colluders*.

3. Adaptive Privacy-Preserving Coded Computing

In this section, we propose the adaptive privacy-preserving coded computing (APCC) strategy, which is suitable for diverse computation tasks including polynomial functions and non-polynomial functions, and can adaptively provide accurate results or approximated results. We begin with a general description to explain how APCC works and then provide an illustrative example for accurate results case without loss of generality. Lastly, we introduce the hierarchical task partitioning structure of APCC, and the cancellation of completed subtasks based on this hierarchical structure.

3.1. General Description

In this subsection, we provide a general description of the proposed APCC strategy. As shown in Figure 2, the inputs of the function f are first equally pre-divided into K parts $\{\mathbf{D}_k\}_{k=0}^{K-1}$, and K corresponding subtasks $\{f(\mathbf{D}_k)\}_{k=0}^{K-1}$ are formed. The APCC strategy then follows three steps: (1) *Encoding*; (2) *Assignment*; (3) *Decoding*, and obtains accurate or approximated computing results of $\{f(\mathbf{D}_k)\}_{k=0}^{K-1}$.

3.1.1. Encoding

In the initialization step, the K subtasks are further partitioned into r sets, with set i ($i \in [0 : r - 1]$) containing K_i subtasks $\{f(\mathbf{D}_{i,j})\}_{j=0}^{K_i-1}$, where $\mathbf{D}_{i,j} \in \{\mathbf{D}_k | k \in [0 : K - 1]\}$. Consequently, the desired results of the master are

$$\{f(\mathbf{D}_k)\}_{k=0}^{K-1} = \left\{ \{f(\mathbf{D}_{i,j})\}_{j=0}^{K_i-1} | i \in [0 : r - 1] \right\}, \tag{1}$$

where K_i should satisfy $\sum_{i=0}^{r-1} K_i = K$. The specific values of $\{K_i\}_{i=0}^{r-1}$ will be formulated as optimization problems in Section 5. We refer to the partition of these sets as *hierarchical task partitioning*.

Inspired by Barycentric polynomial interpolation [27,44], the input data $\{\mathbf{D}_{i,j}\}_{j=0}^{K_i-1}$ for set i is linearly encoded through function $g_i(x)$ as:

$$g_i(x) = \sum_{j=0}^{K_i-1} \frac{w_{i,j} \prod_{k=0, k \neq j}^{K_i+L-1} (x - \alpha_{i,k})}{\sum_{k=0}^{K_i+L-1} w_{i,k} \prod_{l=0, l \neq k}^{K_i+L-1} (x - \alpha_{i,l})} \mathbf{D}_{i,j} + \sum_{j=K_i}^{K_i+L-1} \frac{w_{i,j} \prod_{k=0, k \neq j}^{K_i+L-1} (x - \alpha_{i,k})}{\sum_{k=0}^{K_i+L-1} w_{i,k} \prod_{l=0, l \neq k}^{K_i+L-1} (x - \alpha_{i,l})} \mathbf{Z}_{i,j}, \tag{2}$$

where $\{\mathbf{Z}_{i,j} \in \mathbb{V} | j \in [K_i : K_i + L - 1]\}$ are L random matrices added to preserve the privacy, each element in $\mathbf{Z}_{i,j}$ follows a uniform distribution, and $x \in \mathbb{R}$ is the encoding parameter. $\{\alpha_{i,j}\}_{j=0}^{K_i+L-1}$ are distinct values selected as Chebyshev points of the first kind:

$$\alpha_{i,j} = \cos \frac{(2j + 1)\pi}{2(K_i + L)}, j \in [0 : K_i + L - 1]. \tag{3}$$

$w_{i,j}$ is a constant related to $\alpha_{i,j}$ and calculated as:

$$w_{i,j} = \frac{1}{\prod_{k=0, k \neq j}^{K_i+L-1} (\alpha_{i,j} - \alpha_{i,k})}, j \in [0 : K_i + L - 1]. \tag{4}$$

Note that the form of $g_i(x)$ is a Barycentric polynomial [27,44], which can avoid overflows and underflows in floating-point arithmetic and requires a lower computation

complexity compared to its similar form of Lagrange polynomial in LCC [15]. Furthermore, Equation (2) guarantees that

$$g_i(\alpha_{i,j}) = D_{i,j}, \quad j \in [0 : K_i - 1]. \tag{5}$$

because the coefficient term before $D_{i,j}$ and $Z_{i,j}$

$$\frac{w_{i,j} \prod_{k=0, k \neq j}^{K_i+L-1} (x - \alpha_{i,k})}{\sum_{k=0}^{K_i+L-1} w_{i,k} \prod_{l=0, l \neq k}^{K_i+L-1} (x - \alpha_{i,l})} = \begin{cases} 1, & \text{if } x = \alpha_{i,j}, \\ 0, & \text{if } x = \alpha_{i,k}, k \neq j. \end{cases} \tag{6}$$

The encoded input data $\{\tilde{D}_{i,n}\}_{n=0}^{N-1}$ are obtained as:

$$\tilde{D}_{i,n} = g_i(\beta_n), n \in [0 : N - 1]. \tag{7}$$

$\{\beta_n\}_{n=0}^{N-1}$ are selected as Chebyshev points of the second kind:

$$\beta_n = \cos \frac{n\pi}{N-1}, n \in [0 : N - 1]. \tag{8}$$

3.1.2. Assignment

For set i , the encoded data $\tilde{D}_{i,n} = g_i(\beta_n)$ is assigned to worker n . Consequently, as Figure 2 shows, each worker receives r encoded subtasks $\{f(\tilde{D}_{i,n})\}_{i=0}^{r-1}$ and executes them in the order of set indices. Once completed, the result of each encoded subtask $f(\tilde{D}_{i,n})$ is returned to the master. In other words, after the original K subtasks are partitioned into multiple sets, each set is transformed into N encoded subtasks assigned to N workers for processing.

3.1.3. Decoding

For set i , the master decodes using function $r_i(x)$, which is constructed by interpolation [27,44] as:

$$r_i(x) = \sum_{n=0}^{R_i-1} \frac{\frac{\tilde{w}_n}{x - \tilde{x}_n}}{\sum_{m=0}^{R_i-1} \frac{\tilde{w}_m}{x - \tilde{x}_m}} f(g_i(\tilde{x}_n)), \tag{9}$$

where $\{f(g_i(\tilde{x}_n)) | n \in [0 : R_i - 1]\}$ are the first R_i received results in $\{f(\tilde{D}_{i,n})\}_{n=0}^{N-1}$ for set i , \tilde{x}_n is the corresponding encoding parameter that belongs to $\{\beta_n | n \in [0, N - 1]\}$, and the parameter \tilde{w}_n is adaptive for different cases, as follows.

Case 1: Accurate results. If f is a polynomial function of degree d , where the degree d of a polynomial function is defined as the maximum order of its monomials, the adaptive parameters \tilde{w}_n is determined as:

$$\tilde{w}_n = \frac{1}{\prod_{m=0, m \neq n}^{R_i-1} (\tilde{x}_n - \tilde{x}_m)}, n \in [0 : R_i - 1]. \tag{10}$$

In this case, $r_i(x)$ is a Barycentric polynomial interpolation function [44] for $f(g_i(x))$. The degree of $g_i(x)$ equals $(K_i + L - 1)$, so that $f(g_i(x))$ remains a polynomial function, and its degree satisfies $\deg f(g_i(x)) \leq d(K_i + L - 1)$. Consequently, if the number of received results R_i for set i satisfies:

$$R_i = d(K_i + L - 1) + 1, \tag{11}$$

it implies that sufficient interpolation points have been obtained to precisely recover $f(g_i(x))$ through $r_i(x)$, and the entire computation process is completed with

$$f(\mathbf{D}_{i,j}) = f(g_i(\alpha_{i,j})) = r_i(\alpha_{i,j}), \tag{12}$$

for any $i \in [0 : r - 1], j \in [0 : K_i - 1]$.

Note that Equation (11) means that the accurate result case of APCC has the same recovery threshold as LCC [15]. Furthermore, similar to LCC, when there is no need for privacy preservation, which means $L = 0$, we can also provide an uncoded version of APCC by selecting the value of $\{\beta_n\}$ from $\{\alpha_{i,j}\}$. Thus, the new recovery threshold becomes:

$$R_i = N - \left\lfloor \frac{N}{K_i} \right\rfloor + 1. \tag{13}$$

Case 2: Approximated results. If f is an arbitrary function, the adaptive parameter \tilde{w}_n is calculated as:

$$\tilde{w}_n = (-1)^n, n \in [0 : R_i - 1]. \tag{14}$$

In this case, $r_i(x)$ is a Berrut’s rational interpolation function for $f(g_i(x))$, as discussed in [27,45]. The computed results $f(g_i(\tilde{x}_n))$ serve as the interpolation points of $f(g_i(x))$, and they satisfy $r_i(\tilde{x}_n) = f(g_i(\tilde{x}_n))$ due to the property of Berrut’s rational interpolation [45]. Therefore, the master can regard $r_i(x)$ as an approximation of $f(g_i(x))$, which means that

$$f(\mathbf{D}_{i,j}) = f(g_i(\alpha_{i,j}) \approx r_i(\alpha_{i,j}), \tag{15}$$

for any $i \in [0 : r - 1], j \in [0 : K_i - 1]$. In addition, the approximation using $r_i(x)$ becomes more accurate as R_i increases. Thus, if the master desires more accurate computations, it simply needs to wait for more results.

3.2. An Illustrating Example

In this subsection, we present an illustrative example for the case of accurate results without loss of generality. Specifically, we consider a linear regression problem. The feature data $\mathbf{D} \in \mathbb{R}^{12000 \times 10}$ contains 12,000 data samples with 10 features, and the label vector is denoted by $\mathbf{y} \in \mathbb{R}^{12000 \times 1}$. The objective is to find the weighting vector $\mathbf{w} \in \mathbb{R}^{10 \times 1}$ that minimizes the loss $\|\mathbf{D}\mathbf{w} - \mathbf{y}\|^2$. To solve this problem, the gradient descent method updates the weights iteratively along the negative gradient direction as follows:

$$\mathbf{w}^{(t+1)} = \mathbf{w}^{(t)} - \frac{2\eta}{p'} \mathbf{D}^T (\mathbf{D}\mathbf{w}^{(t)} - \mathbf{y}), \tag{16}$$

where η is the learning rate and t represents the iteration index.

In order to apply the aforementioned update process to a distributed system with one master and $N = 10$ workers, for instance, the feature data \mathbf{D} is first equally divided into $K = 12$ sub-matrices $(\mathbf{D}_0, \mathbf{D}_1, \dots, \mathbf{D}_{11})^T, \mathbf{D}_k \in \mathbb{R}^{1000 \times 10}, k \in [0 : 11]$. As $\mathbf{w}^{(t)}$ is known by the workers and $\mathbf{D}^T \mathbf{y}$ can be precomputed by the master, the computation function (subtask) of the master in each iteration can be expressed as $f(\mathbf{D}_k) = \mathbf{D}_k^T \mathbf{D}_k \mathbf{w} \in \mathbb{R}^{10 \times 1}, k \in [0 : 11]$. After obtaining the results of the entire task $\{f(\mathbf{D}_k)\}_{k=0}^{11}$, the gradient update is computed as $\mathbf{D}^T \mathbf{D}\mathbf{w} = \sum_{k=0}^{11} \mathbf{D}_k^T \mathbf{D}_k \mathbf{w}$.

We now illustrate how APCC can be applied in the above problem, to obtain $f(\mathbf{D}_k) = \mathbf{D}_k^T \mathbf{D}_k \mathbf{w}, k \in [0 : 11]$.

3.2.1. Encoding

As depicted in Figure 3a, since there are 12 subtasks $f(\mathbf{D}_k), k \in [0 : 11]$, the master further partitions them into $r = 3$ sets before encoding input data, and set $i (i = 0, 1, 2)$ contains K_i subtasks. Here, for instance, we assume that $K_0 = 5, K_1 = 4$, and $K_2 = 3$, and

they satisfy $K_0 + K_1 + K_2 = K = 12$. After this hierarchical task partitioning, the input of the j -th subtask in set i is denoted as $D_{i,j} \in \mathbb{R}^{1000 \times 10}$ instead of the previous D_k .

Next, the K_i input data $\{D_{i,j} \in \mathbb{R}^{1000 \times 10} | j = 0, \dots, K_i - 1\}$ in set i are encoded into $N = 10$ parts $\{\tilde{D}_{i,n} \in \mathbb{R}^{1000 \times 10} | n = 0, \dots, 9\}$ through $g_i(x)$, where $\tilde{D}_{i,n} = g_i(\beta_n), n \in [0 : 9]$. Moreover, $g_i(x)$ is a polynomial function with a degree of $(K_i + L - 1)$, and its form ensures that the parameters $\{\alpha_{i,j}\}$ satisfy $g_i(\alpha_{i,j}) = D_{i,j}$.

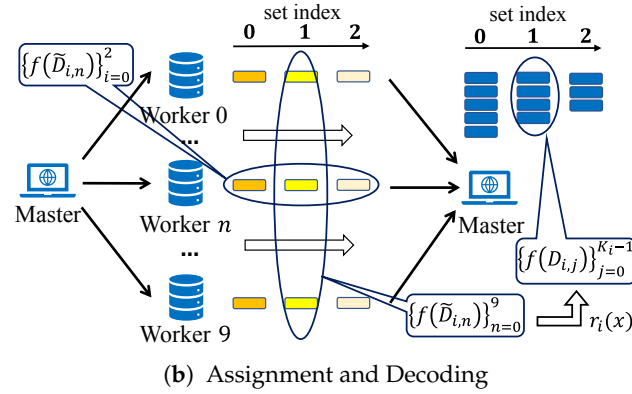
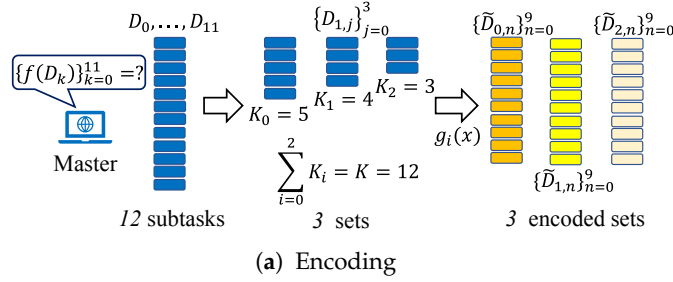


Figure 3. The three-step process of APCC.

3.2.2. Assignment

As Figure 3b shows, for each set, the 10 encoded input data $\{\tilde{D}_{i,n}\}_{n=0}^9$ are assigned to the 10 workers. Subsequently, each worker applies function f to compute and return the results to the master. As can be observed, the K_i original subtasks in set i are transformed into 10 subtasks performed on the 10 workers in parallel. Since there are 3 sets, each worker is assigned 3 subtasks. These subtasks are executed in the order of set indices, which implies $f(\tilde{D}_{0,n})$ is computed first, followed by $f(\tilde{D}_{1,n})$, and so on.

3.2.3. Decoding

As illustrated in Figure 3b, following the assignment of encoded input to workers, the master continuously awaits the subtask results from workers and creates a decoding function $r_i(x)$ for set i . This decoding function is constructed using interpolation to recover the original function $f(D_{i,j}) = f(g_i(\alpha_{i,j}))$. Consequently, each received result, $f(g_i(\beta_n))$, can be regarded as an interpolation point for $f(g_i(x))$, and $r_i(x)$ is precisely the interpolation function of $f(g_i(x))$.

Presently, $f(D_{i,j}) = D_{i,j}^T D_{i,j} w$ is a polynomial function of degree $d = 2$, where the degree d of a polynomial function f is defined as the maximum order of its monomials. We have illustrated how to complete the decoding process in Subsection III.A. By setting the number of received results to $R_i = d(K_i + L - 1) + 1$, sufficient interpolation points are obtained to accurately recover $f(g_i(x))$ through $r_i(x)$, i.e., $f(D_{i,j}) = f(g_i(\alpha_{i,j})) = r_i(\alpha_{i,j})$, for any $i \in [0 : 2]$ and $j \in [0 : K_i - 1]$. To further illustrate APCC, we also provide a corresponding pseudo-code, as presented in Algorithm 1.

Algorithm 1: APCC

Input: f, D_k, r, K_i, N, L
Output: $\{f(D_k)\}_{k=0}^{K-1}$.

- 1 **(1) Encoding:**
- 2 The master partitions K subtasks $\{f(D_k)\}_{k=0}^{K-1}$ into r sets, and set i consists of K_i subtasks $\{f(D_{i,j})\}_{j=0}^{K_i-1}$;
- 3 **for** $i = 0 : r - 1$ **do**
- 4 The master encodes $\{D_{i,j}\}_{j=0}^{K_i-1}$ into $\{\tilde{D}_{i,n}\}_{n=0}^{N-1}$ according to $\tilde{D}_{i,n} = g_i(\beta_n)$ through Barycentric polynomial, similar to the Lagrange polynomial of LCC;
- 5 **(2) Assignment:**
- 6 **for** $n = 0 : N - 1$ **do**
- 7 The master assigns $\{\tilde{D}_{i,n}\}_{i=0}^{r-1}$ to worker n , and $\{f(\tilde{D}_{i,n})\}_{i=0}^{r-1}$ are computed in the order of set indices;
- 8 Workers return $f(\tilde{D}_{i,n})$ to the master once completing computation;
- 9 **(3) Decoding:**
- 10 **for** $i = 0 : r - 1$ **do**
- 11 The master decodes for set i according to the first R_i received results;
- 12 **if** f is a polynomial function of degree d **then**
- 13 Accurate results: $f(g_i(x)) = r_i(x)$, $r_i(x)$ is obtained from Barycentric polynomial interpolation, similar to the Lagrange polynomial interpolation of LCC;
- 14 **if** f is an arbitrary function **then**
- 15 Approximated results: $f(g_i(x)) \approx r_i(x)$, $r_i(x)$ is obtained from Berrut's rational interpolation;
- 16 Set i is completed with $f(D_{i,j}) = f(g_i(\alpha_{i,j}))$;

3.3. Hierarchical Task Partitioning and Cancellation

In Figure 3, the hierarchical task partitioning in APCC aims to maximize the utility of computing results from straggling workers. This is achieved through a well-designed structure and appropriate choice of K_i values. Although the same number of encoded subtasks are assigned to all workers, the number of successfully returned results from each worker can differ due to varying processing speeds. As a result, straggling workers may return fewer computing results than faster workers, but they can still make valuable contributions to task completion instead of being completely discarded.

Furthermore, the illustration in Figure 3 suggests that K_{i-1} should exceed K_i [11]. This assertion is explained as follows: The “completion time” of set i is defined as the moment when a sufficient number of encoded subtask results within set i are obtained. The overarching objective is to minimize the delay in completing the entire task, which must necessarily exceed the “completion time” of any set since the entire task remains incomplete until all r sets are recovered. Given that subtasks are executed in order of set indices, when set r is recovered, the master must have acquired results for the smaller-index sets equal to or greater than K_i . Opting for smaller values of K_i for the smaller-index sets would result in more workers experiencing straggling, a situation that should be averted. Further details are expounded in Section 5.

Based on the hierarchical structure, we propose an alternative method to further accelerate the coded computing process. As depicted in Figure 4, the subtasks $\{f(\tilde{D}_{i,n})\}_{i=0}^{r-1}$ to be computed on each worker form an execution sequence. Once enough results for set i are obtained, the master can instruct workers that have not completed the computation of $f(\tilde{D}_{i,n})$ to terminate or skip this part of the computation and proceed to compute the next subtasks $f(\tilde{D}_{i+1,n})$ of the subsequent set. This operation, called “Cancellation”, prevents

computation resources from being wasted on completed sets. Considering the presence of non-persistent stragglers, cancellation increases the probability of them overcoming the previous straggling effect and avoiding becoming stragglers again.

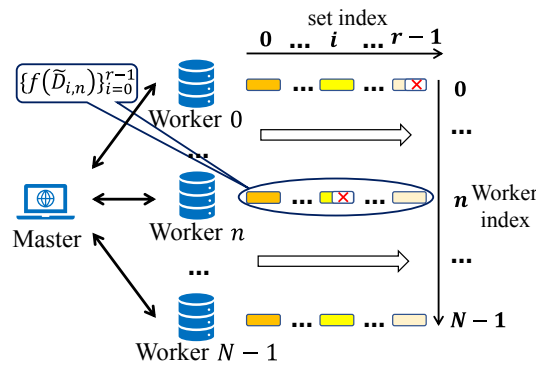


Figure 4. Hierarchical structure and the cancellation operation.

4. Performance Analysis

In this section, we first define a metric called *encoding rate* to evaluate the efficiency performance of coded computing schemes, in terms of utilizing computation resources of workers as efficiently as possible. Then, based on the optimal recovery threshold of LCC [15], we rigorously prove APCC for accurate results is also an optimal polynomial coding in terms of the encoding rate. Furthermore, an information-theoretic guarantee to completely preserve the privacy of input data $\{D_k\}_{k=0}^{K-1}$ in APCC is proved. Subsequently, we present an analysis of the approximation error for Case 2 of APCC, along with a discussion of numerical stability. At the end of this section, we provide an analysis of encoding and decoding complexity for APCC and compare it with other state-of-the-art strategies.

4.1. Optimality of APCC in Terms of Encoding Rate

To evaluate the performance of various coded computing schemes, a metric known as the encoding rate R_{encode} is used. This metric is defined as:

$$R_{\text{encode}} = \frac{K}{N - S}, \tag{17}$$

where K is the number of subtasks before encoding, N is the number of subtasks after encoding (which is equivalent to the number of workers), and S represents the number of straggling workers that failed to return results before the task was completed. Similar metrics, such as those found in [17,20,46], have also been developed.

Furthermore, since the recovery threshold, denoted by H , is defined as the minimum number of results needed to guarantee decodability, we have $H = N - S$ and thus $R_{\text{encode}} = \frac{K}{H}$. It is important to note that the encoding rate only applies when decodability is guaranteed.

The physical significance of the encoding rate is the ratio between the computation load of tasks before encoding and that required after encoding. For instance, given a task with a computation load of $O(\gamma)$, each subtask has a corresponding load of $O(\frac{\gamma}{K})$. As $(N - S)$ subtasks are successfully completed, the required computation load is $O(\frac{\gamma(N-S)}{K})$. Since coded computing essentially trades computation redundancy for reduced delay to mitigate the straggling effect, it is reasonable to use this metric to evaluate the efficiency of different schemes.

Before demonstrating the optimality of APCC in terms of encoding rate, we present the definitions of capacity and linear coded computing schemes.

Definition 1. A linear coded computing scheme is one in which the encoded data is a linear combination of the original input data as follows:

$$\tilde{D}_n = \sum_{j=0}^{K-1} G_{n,j} D_j + \tilde{Z}_n, n \in [0 : N - 1], \tag{18}$$

where $G = \{G_{n,j}\} \in \mathbb{R}^{N \times K}$ is the encoding matrix and \tilde{Z}_n are additive random real matrices.

For example, according to Equation (2) in APCC, $G_{n,j} = \frac{w_{i,j} \prod_{k=0, k \neq j}^{K_i+L-1} (\beta_n - \alpha_{i,k})}{\sum_{k=0}^{K_i+L-1} w_{i,k} \prod_{l=0, l \neq k}^{K_i+L-1} (\beta_n - \alpha_{i,l})}$ are the coefficient terms before $D_{i,j}$, and $\tilde{Z}_n = \sum_{j=K_i}^{K_i+L-1} \frac{w_{i,j} \prod_{k=0, k \neq j}^{K_i+L-1} (\beta_n - \alpha_{i,k})}{\sum_{k=0}^{K_i+L-1} w_{i,k} \prod_{l=0, l \neq k}^{K_i+L-1} (\beta_n - \alpha_{i,l})} Z_{i,j}$ represents the sum of added random matrices in $g_i(x)$. The index i corresponds to the set index of the hierarchical task partitioning structure of APCC and can be discarded in other coded computing strategies.

Definition 2. For a coded computing problem (N, S, L, f) , where N is the number of workers, S and L denote the number of stragglers and colluders, respectively, and the computation function f on the master is a polynomial function of degree d , the capacity C is defined as the supremum of the encoding rate R_{encode} as:

$$C = \sup R_{\text{encode}}(N, S, L, d), \tag{19}$$

over all feasible linear coded computing schemes that can address up to L colluders and S stragglers.

As illustrated in Section 3, APCC is a linear coded computing scheme and its hierarchical structure results in different K_i and S_i for each set, with K_i and S_i representing the number of subtasks before encoding and that of straggling workers, respectively. For set i , R_i represents the number of workers that have successfully returned results in time, implying that the number of stragglers is $S_i = N - R_i$. Moreover, according to Equation (11), set i is considered complete when $R_i = d(K_i + L - 1) + 1$. Hence, the encoding rate of APCC can be calculated as:

$$R_{\text{encode}}^{[\text{APCC}]} = \frac{K_i}{N - S_i} = \frac{N - S_i - d(L - 1) - 1}{d(N - S_i)}, \tag{20}$$

or the uncoded version for $L = 0$:

$$R_{\text{encode}}^{[\text{APCC}]} = \frac{K_i}{N - S_i} \leq \frac{N}{(N - S_i)(S_i + 1)}, \tag{21}$$

where the equality holds when N can be divided by K_i .

The following theorem shows that the encoding rate of APCC achieves the capacity, thereby establishing its optimality. In fact, the optimality of APCC in encoding rate is attributed to its identical polynomial coding structure when compared to LCC [15], despite having different function expressions. Specifically, for the accurate results case of APCC, the encoding and decoding processes are achieved through Barycentric polynomial interpolation; for LCC, the processes are achieved through Lagrange polynomial interpolation. Although these two formats can be transformed into each other, the Barycentric polynomial format requires less computational complexity and has stronger numerical stability [27,44]. For the sake of clarity, we omit the set index i in APCC and focus on a specific set, without loss of generality.

Theorem 1. For a coded computing problem (N, S, L, f) , where N is the number of workers, S and L denote the number of stragglers and colluders, respectively, and the computation function f on the master is an arbitrary polynomial function of degree d , the capacity C is given by:

$$C = \begin{cases} \frac{N-S-d(L-1)-1}{d(N-S)}, & \text{if } L > 0, \\ \max\{\frac{N-S+d-1}{d(N-S)}, \frac{N}{(N-S)(S+1)}\} & \text{if } L = 0. \end{cases} \quad (22)$$

Proof. To prove Theorem 1, a lower bound on the capacity C is first established, which follows the encoding rate of APCC in (20) and (21). To establish the upper bound, we leverage the optimality statement of LCC, as illustrated in Theorems 1 and 2 of [15], which shows that polynomial coded computing strategies are able to decode returned computing results successfully only if the following condition is met:

$$N \geq \begin{cases} d(K + L - 1) + 1 + S, & \text{if } L > 0, \\ \min\{d(K - 1) + 1 + S, K(S + 1)\} & \text{if } L = 0. \end{cases} \quad (23)$$

Therefore, we have:

$$K \leq \begin{cases} \frac{N-S-1}{d} - L + 1, & \text{if } L > 0, \\ \max\{\frac{N-S+d-1}{d}, \frac{N}{(S+1)}\} & \text{if } L = 0. \end{cases} \quad (24)$$

Equation (24) presents the maximum number of task divisions permissible to ensure decodability, given the numbers of workers N , stragglers S , and colluders L . The reason is that the more divisions there are, the more results are needed from workers. However, there are at most N workers, including S stragglers, to return results. Based on (24), an upper bound on the encoding rate can be derived as:

$$R_{\text{encode}} = \frac{K}{N-S} \leq \begin{cases} \frac{N-S-d(L-1)-1}{d(N-S)}, & \text{if } L > 0, \\ \max\{\frac{N-S+d-1}{d(N-S)}, \frac{N}{(N-S)(S+1)}\} & \text{if } L = 0. \end{cases} \quad (25)$$

Since the capacity C is the supremum of R_{encode} , it also has the same upper bound. With the lower bound provided previously, we can conclude that APCC is an optimal coded computing strategy that can reach the capacity in (22). \square

To enhance clarity, the fundamental proof for the derivation of (23) is briefly introduced in Appendix A, following the same steps as outlined in [15].

Please note that the conclusion presented in this subsection pertains only to accurately coded computing. For approximated coded computing, the use of different approximation methods can lead to varying errors, making it challenging to compare and analyze their impact on the encoding rate and capacity in a qualitative manner.

4.2. Guarantee of the Privacy Preservation

Recall that colluders are those workers who can communicate with each other and attempt to learn something about the original input data. Since the system can tolerate at most L colluders, we assume that there are L' colluders, where $L' \leq L$ and the user does not know which workers are colluding. We use the index set $\mathcal{L} = \{l_0, l_1, \dots, l_{L'-1}\} \subseteq \{0, \dots, N - 1\}$ to denote the colluding workers, where $|\mathcal{L}| = L'$.

Assuming that the input data $\{D_{i,j}\}_{j=0}^{K_i-1}$ are independent of each other, we denote the encoded input data sent to workers in the colluding set \mathcal{L} for set i as:

$$\tilde{D}_{i,\mathcal{L}} \triangleq (\tilde{D}_{i,l_0}, \tilde{D}_{i,l_1}, \dots, \tilde{D}_{i,l_{L'-1}}). \quad (26)$$

Therefore, the information-theoretic privacy-preserving constraint can be expressed as:

$$I(\mathbf{D}_{i,0}, \mathbf{D}_{i,1}, \dots, \mathbf{D}_{i,K_i-1}; \tilde{\mathbf{D}}_{i,\mathcal{L}}) = 0, \forall i \in [0, r - 1], \tag{27}$$

where $I(\cdot)$ represents the mutual information function.

With the assumption of finite precision floating point arithmetic, the values of elements in the data matrices such as $\mathbf{D}_{i,j}$, $\tilde{\mathbf{D}}_{i,n}$, and $\mathbf{Z}_{i,j}$ come from a sufficiently large finite field \mathbb{F} . Assuming that the size of these data matrices is $m \times m'$, we have

$$\begin{aligned} I(\mathbf{D}_{i,0}, \mathbf{D}_{i,1}, \dots, \mathbf{D}_{i,K_i-1}; \tilde{\mathbf{D}}_{i,\mathcal{L}}) &= H(\tilde{\mathbf{D}}_{i,l_0}, \dots, \tilde{\mathbf{D}}_{i,l_{L-1}}) \\ &\quad - H(\tilde{\mathbf{D}}_{i,l_0}, \dots, \tilde{\mathbf{D}}_{i,l_{L-1}} | \mathbf{D}_{i,0}, \dots, \mathbf{D}_{i,K_i-1}) \\ &\stackrel{(a)}{=} H(\tilde{\mathbf{D}}_{i,l_0}, \dots, \tilde{\mathbf{D}}_{i,l_{L-1}}) - H(\mathbf{Z}_{i,K_i}, \dots, \mathbf{Z}_{i,K_i+L-1}) \\ &\stackrel{(b)}{=} H(\tilde{\mathbf{D}}_{i,l_0}, \dots, \tilde{\mathbf{D}}_{i,l_{L-1}}) - Lmm' \log |\mathbb{F}| \\ &\leq H(\tilde{\mathbf{D}}_{i,l_0}) + \dots + H(\tilde{\mathbf{D}}_{i,l_{L-1}}) - Lmm' \log |\mathbb{F}| \\ &\stackrel{(c)}{\leq} L'mm' \log |\mathbb{F}| - Lmm' \log |\mathbb{F}| = 0, \forall i \in [0, r - 1], \end{aligned} \tag{28}$$

where (a) is due to the fact that all random matrices $\{\mathbf{Z}_{i,j}\}_{j=K_i}^{K_i+L-1}$ are independent of the input data $\{\mathbf{D}_{i,j}\}_{j=0}^{K_i-1}$. (b) is because the entropy of each element in the random matrices equals $\log |\mathbb{F}|$, and (c) follows from the upper bound of the entropy of each element in $\tilde{\mathbf{D}}_{i,l(\cdot)}$ being $\log |\mathbb{F}|$. Since the mutual information is non-negative, it must be 0, which guarantees complete privacy preservation.

Note that the analysis in this subsection is applicable to both accurate and approximated cases. This is because the analysis only involves the encoding and assignment steps of APCC, and both cases require the same two initial steps. The key difference between the two aforementioned cases is reflected in the decoding functions with distinct adaptive parameters \tilde{w}_n , which correspond to Barycentric polynomial interpolation and Berrut's rational interpolation, respectively.

4.3. Analysis of Approximation Error for Case 2

According to the discussion in [27], the approximation error of Berrut's rational polynomial interpolation used for Case 2 in APCC is provided as the following theorem:

Theorem 2 ([27]). *Let the interpolating objective function $h_i(x) = f(g_i(x))$ have a continuous second derivative on $[-1, 1]$, and the number of received results $R_i > 3$, the approximation error is upper bounded as:*

$$\begin{aligned} \|r_i(x) - h_i(x)\| &\leq \\ &2(1 + \Gamma) \sin \frac{(N - R_i + 1)\pi}{2(N - 1)} \|h_i''(x)\|, \end{aligned} \tag{29}$$

if R_i is even, and

$$\begin{aligned} \|r_i(x) - h_i(x)\| &\leq \\ &2(1 + \Gamma) \sin \frac{(N - R_i + 1)\pi}{2(N - 1)} (\|h_i''(x)\| + \|h_i'(x)\|), \end{aligned} \tag{30}$$

if R_i is odd, where $\Gamma \triangleq \frac{(N-R_i+1)(N-R_i+3)\pi^2}{4}$.

Consequently, for set i and a fixed total number of workers N , the approximation using $r_i(x)$ becomes more accurate as the number of received results R_i increases.

4.4. Numerical Stability

In coded computing, the issue of numerical stability typically arises from the decoding part, which is based on solving a system of linear equations involving a Vandermonde matrix. As previously discussed, Cases 1 and 2 of APCC employ Barycentric polynomial interpolation and Berrut's rational interpolation as decoding methods, respectively. For Case 1, Barycentric polynomial interpolation demonstrates good performance in addressing errors caused by floating-point arithmetic [44]. Regarding Case 2, it has been shown in [27] that the Lebesgue Constant of Berrut's rational interpolation grows logarithmically with the number of received results from workers, rendering it both forward and backward stable.

4.5. Encoding and Decoding Complexity

In this subsection, we provide the analysis of encoding and decoding complexity. Intuitively, APCC utilizes the hierarchical task partitioning structure to enhance delay performance. However, it does so at the cost of requiring multiple encoding and decoding operations, specifically r times for the r sets, when compared to LCC [15] and BACC [27].

In LCC and BACC, the encoding operations take N times, corresponding to the number of workers, while the decoding operations take K' times, equivalent to the number of task divisions. On the other hand, in the case of APCC, which features r partitioned sets, the encoding and decoding operations entail Nr and $\sum_{i=0}^r K_i = K$, respectively. When the computation loads per worker in all strategies are equal, i.e., $K' = \frac{K}{r}$, it can be deduced that the encoding and decoding operations in APCC are r times those of LCC and BACC.

5. Hierarchical Task Partitioning

In this section, the hierarchical task partitioning is formulated as an optimization problem with the objective of minimizing the task completion delay. The problem is divided into two cases for consideration: with and without cancellation. Through derivations, two mixed integer non-linear programming problems are obtained, and we propose a maximum value descent (MVD) algorithm to obtain the optimal solutions with low computational complexity. Moreover, after analysis, it is found that the MVD algorithm can be quickly executed by selecting the appropriate input. Detailed explanations are provided as follows.

5.1. Problem Formulation

In the context of negligible encoding and decoding delays, with the computation delays of workers being the dominant component, the delay for a worker to complete a single sub-task, denoted as T can be represented by a shifted exponential distribution [4,7,11,12,40,41], whose cumulative distribution function (CDF) is given by:

$$F_T(t) = \mathbb{P}[T \leq t] = \begin{cases} 1 - e^{-\mu(t-a)}, & \text{if } t \geq a, \\ 0, & \text{otherwise,} \end{cases} \quad (31)$$

where $a > 0$ is a parameter indicating the minimum processing time and $\mu > 0$ is a parameter modeling the computing performance of workers. All N workers follow a uniform computation delay distribution defined in (31).

Recall that in the hierarchical structure, the completion of a particular set is dependent on the successful receiving of a sufficient number of results from its encoded subtasks. The overall completion of the entire task is achieved only when all r sets have been completed. Notably, H_i is defined as the threshold number of successful results needed to ensure the completion of set i .

Following the discussion in Section 3 and assuming that privacy preservation is required which means $L > 0$, the threshold for Case 1 of APCC can be expressed as $H_i = d(K_i + L - 1) + 1$ according to (11). For Case 2 of APCC, the threshold H_i can be determined based on the desired approximation precision, with higher values of H_i leading to more accurate approximations.

The completion time of sets is defined as $t \triangleq \{t_i, i \in [0 : r - 1]\}$, where t_i denotes the time interval from the initial moment 0 of the entire task to the recovery moment of set i . The entire task is considered completed when all r sets have been recovered. Therefore, we denote the entire task completion delay as

$$T^{[e]} = \max_{i \in [0:r-1]} t_i. \tag{32}$$

Note that while each worker executes the assigned subtasks in the order of set indices, the order in which these sets are recovered may not be the same. The completion time of sets is influenced not only by the set indices but also by the recovery thresholds H_i determined by K_i .

Due to the randomness of delay, our objective is to minimize the entire task completion delay $T^{[e]} = \max_{i \in [0:r-1]} t_i$, upon which the probability of the master recovering desired results for all sets is higher than a given threshold ρ_s , as expressed by the following inequality:

$$\mathbb{P}[R_0(t_0) \geq H_0, \dots, R_{r-1}(t_{r-1}) \geq H_{r-1}] \geq \rho_s, \tag{33}$$

where $R_i(t)$ is defined as the number of returned results for set i until time t .

However, to derive (33), we first need to obtain the distribution of the delay required to receive the last non-straggling result in each set and then derive their joint probability distribution, which is intractable, especially when considering the cancellation of completed sets. As a result, the problem with the constraint (33) is hard to solve.

In the following, we consider substituting (33) with an expectation constraint (34d) and formulate the problem as:

$$\mathcal{P1} - 1 : \min_{\{K\}} \max_{i \in [0:r-1]} t_i \tag{34a}$$

$$\text{s.t. } \sum_{i=0}^{r-1} K_i = K, \tag{34b}$$

$$H_i \leq N, \forall i \in [0, r - 1] \tag{34c}$$

$$\mathbb{E}[R_i(t_i)] \geq H_i, \forall i \in [0, r - 1] \tag{34d}$$

$$K_i, H_i \in \mathbb{Z}^+, \forall i \in [0, r - 1], \tag{34e}$$

where $K \triangleq \{K_i | i \in [0 : r - 1]\}$ is the partitioning scheme.

Constraint (34b) corresponds to the hierarchical task partitioning, and (34c) indicates that the threshold for each set should be smaller than the number of workers. In constraint (34e), \mathbb{Z}^+ represents the set of positive integers. Constraint (34d) states that the master is expected to receive sufficient results of encoded subtasks from workers to recover $f(\mathbf{D}_{i,j})_{j=0}^{K_i-1}$ in set i . Similar approximation approaches are also used in [4,12,40,41], and the performance gap can be bounded [12].

As previously shown, $H_i = d(K_i + L - 1) + 1$ for Case 1 of APCC. Additionally, the maximum of t_i for all sets can be replaced with an optimization variable z by adding an extra constraint. Consequently, for Case 1 of APCC, $\mathcal{P1} - 1$ can be equivalently written as:

$$\mathcal{P1} - 2 : \min_{\{K,z\}} z \tag{35a}$$

$$\text{s.t. } t_i - z \leq 0, \forall i \in [0, r - 1], \tag{35b}$$

$$d(K_i + L - 1) + 1 - \mathbb{E}[R_i(t_i)] \leq 0, \forall i \in [0, r - 1], \tag{35c}$$

$$d(K_i + L - 1) + 1 - N \leq 0, \forall i \in [0, r - 1], \tag{35d}$$

$$K_i \in \mathbb{Z}^+, \forall i \in [0, r - 1], \tag{35e}$$

$$\text{Constraint (34b)}. \tag{35f}$$

For Case 2 of APCC, one only needs to adjust constraints (35c) and (35d) according to the relationship between K_i and H_i , which does not affect the subsequent methods employed. Consequently, for the sake of convenience in expression, we will focus on Case 1 of APCC in the following parts of this section, without loss of generality.

5.2. APCC without Cancellation

If the cancellation of completed sets is not considered, we first denote the delay of one worker to continuously complete m subtasks as T_m , and derive its CDF from (31) as:

$$\mathbb{P}[T_m \leq t] = \begin{cases} 1 - e^{-\mu(\frac{t}{m}-a)}, & \text{if } t \geq ma, \\ 0 & \text{otherwise.} \end{cases} \tag{36}$$

Since computations on workers are independent, $\mathbb{E}[R_i(t_i)]$ can be written as:

$$\mathbb{E}[R_i(t_i)] = \sum_{n=0}^{N-1} \mathbb{E}[\mathbb{I}_{\{T_{i+1} \leq t_i\}}] = N \cdot \mathbb{P}[T_{i+1} \leq t_i], \tag{37}$$

where $\mathbb{I}_{\{x\}}$ denotes the indicator function that equals 1 if event x is true and equals 0 otherwise. $\mathbb{P}[T_{i+1} \leq t_i]$ is given by (36).

Substituting (37) into P1 – 2, we find (35d) is covered by (35c) and obtain the following optimization problem:

$$\mathcal{P}2 - 1 : \min_{\{K,z\}} z \tag{38a}$$

$$\begin{aligned} \text{s.t. } & d(K_i + L - 1) + 1 - N[1 - e^{-\mu(\frac{t_i}{i+1}-a)}] \leq 0, \\ & \forall i \in [0, r - 1], \end{aligned} \tag{38b}$$

$$\text{Constraints (34b), (35b), (35e).} \tag{38c}$$

As P2 – 1 shows, it is a mixed integer non-linear programming (MINLP) problem, which is usually NP-hard. Although its optimal solution can be found by the Branch and Bound (B&B) algorithm [47], the computational complexity is up to $O\left(\left(\frac{N}{d}\right)^r\right)$, which means the B&B algorithm becomes extremely time-consuming when either N or r are large.

Accordingly, to efficiently obtain an optimal solution, we propose the maximum value descent (MVD) algorithm shown in Algorithm 2. The key idea of the MVD algorithm is to iteratively update the input solution $K = \{K_i, i \in [0 : r - 1]\}$ by adjusting K_i for the set that corresponds to the maximum value descent of the objective function z . In the MVD algorithm, each do-while loop can be regarded as one update, and K_j in Step 7 constantly approaches the optimal K_j^* . Once reduced in an update, K_j will not increase because the objective function z must decrease in each update. When the updating process terminates, the optimal solution K^* is exactly the obtained K in the last update. Furthermore, the MVD algorithm has a computational complexity of $O\left(\frac{Nr}{d}\right)$, as the number of do-while loops is determined by constraint (35d).

Furthermore, the MVD algorithm can be executed quickly by selecting a sufficiently good partitioning solution as input. It should be noted that after relaxation and cancellation of the integer constraint in (35e), P2 – 1 can be transformed into a convex problem as follows:

$$\mathcal{P}2 - 2 : \min_{\{K,z\}} z \tag{39a}$$

$$\text{s.t. Constraints (38b), (34b), (35b),} \tag{39b}$$

$$K_i > 0, \forall i \in [0, r - 1]. \tag{39c}$$

and the optimal solution is given in Proposition 1 according to the Karush–Kuhn–Tucker (KKT) conditions.

Algorithm 2: MVD

Input: An arbitrary feasible solution: $\mathbf{K} = \{K_i, i \in [0, r - 1]\}$
Output: The optimal solution: $\mathbf{K}^* = \{K_i^*, i \in [0, r - 1]\}$

- 1 **do**
- 2 Substitute \mathbf{K} into the original problem and obtain the following convex optimization problem.

$$\mathcal{P} : \min_{\{t, z\}} z \quad \text{s.t. (35b), (38b).}$$
- 3 Obtain the solution $\{t^*, z^*\}$ to \mathcal{P} by solving the Karush–Kuhn–Tucker (KKT) conditions.
- 4 Derive $z^* = \max_{i \in [0:r-1]} t_i^*$ and assume $t_j^* = z^*, j \in [0 : r - 1]$ without loss of generality.
- 5 Initialization: $\mathbf{K}^{MVD} = \mathbf{K}$ and $z^{MVD} = z^*$.
- 6 **for** $l = [0 : r - 1], l \neq j$ **do**
- 7 $\mathbf{K}^{temp} = \mathbf{K}, K_j^{temp} = K_j - 1, K_l^{temp} = K_l + 1.$
- 8 Substitute \mathbf{K}^{temp} into the original problem and obtain the corresponding z^{temp} like Step 2-3.
- 9 **if** $z^{temp} < z^{MVD}$ **then**
- 10 $\mathbf{K}^{MVD} = \mathbf{K}^{temp}, z^{MVD} = z^{temp}.$
- 11 $\mathbf{K} = \mathbf{K}^{MVD}.$
- 12 **while** $z^{MVD} < z^*;$

Result: $\mathbf{K}^* = \mathbf{K}$ is the optimal solution.

Proposition 1. For given (N, K, L, d, r, μ, a) , the optimal solution $\mathbf{K}^{[Prop1]}$ and corresponding delay $t^{[Prop1]}$ to $\mathcal{P}2 - 2$ are

$$\sum_{i=0}^{r-1} e^{-\mu(\frac{z^*}{i+1} - a)} = r - \frac{d(K+rL-r)+r}{N}, \tag{40}$$

$$t_i^{[Prop1]} = z^*, K_i^{[Prop1]} = \frac{N}{d} [1 - e^{-\mu(\frac{z^*}{i+1} - a)}] - \frac{1}{d} - L + 1.$$

Due to the convexity of $\mathcal{P}2 - 2$, the Euclidean distance between $\mathbf{K}^{[Prop1]}$ and the optimal solution \mathbf{K}^* of $\mathcal{P}2 - 1$ is small. Therefore, it is recommended to use a rounded result of $\mathbf{K}^{[Prop1]}$ as the input for the MVD algorithm.

5.3. APCC with Cancellation

If the cancellation of completed sets is considered, a worker may be canceled in a certain set but successfully return results in time for the subsequent sets. For example, worker n may be a straggler for set i but completes its assigned subtask and returns the result in time for the next set $(i + 1)$ due to the cancellation. Such situations make it quite difficult to derive and analyze the expectation of $R_i(t)$ as in the previous Section 5.2, because the impact of the cancellation of the previous set on the delay of non-straggling workers in subsequent sets needs to be considered. Therefore, we provide the following alternative perspective to simplify this problem.

Note that if set i is the last completed one, the entire task is completed when the last needed result for this set is received. Thus, we define the delay of set i as $T_i^{[e]}$ and aim to minimize $\max_{i \in [0:r-1]} \mathbb{E}[T_i^{[e]}]$. To derive $\mathbb{E}[T_i^{[e]}]$, consider that there are still $N - H_i + 1 = N - d(K_i + L - 1)$ workers computing the last result for set i when other sets are finished.

Once any one of these workers returns the first result, this set and the entire task will be completed. Accordingly, the CDF of $T_i^{[e]}$ can be written as follows:

$$\begin{aligned} \mathbb{P}\left[T_i^{[e]} \leq t\right] &= 1 - (1 - \mathbb{P}[T_{i+1} \leq t])^{N-d(K_i+L-1)} \\ &= \begin{cases} 1 - e^{-\mu(N-d(K_i+L-1))\left(\frac{t}{i+1}-a\right)}, & \text{if } t \geq (i+1)a, \\ 0 & \text{otherwise,} \end{cases} \end{aligned} \tag{41}$$

where T_{i+1} is the delay needed to complete $(i+1)$ subtasks for one worker, shown previously in (36). Then we have

$$\mathbb{E}[T_i^{[e]}] = \frac{i+1}{\mu[N-d(K_i+L-1)]} + a(i+1). \tag{42}$$

By further adding an extra optimization variable z to substitute $\max_{i \in [0:r-1]} \mathbb{E}[T_i^{[e]}]$, the optimization problem can be formulated as:

$$\mathcal{P}3 - 1 : \min_{\{K,z\}} z \tag{43a}$$

$$\begin{aligned} \text{s.t. } & \frac{i+1}{\mu[N-d(K_i+L-1)]} + a(i+1) - z \leq 0, \\ & \forall i \in [0:r-1], \end{aligned} \tag{43b}$$

$$\text{Constraints (34b), (35d), (35e)}. \tag{43c}$$

Note that $\mathcal{P}3 - 1$ is a MINLP problem similar to $\mathcal{P}2 - 1$ and has an $O\left(\left(\frac{N}{d}\right)^r\right)$ computational complexity to solve if using B&B algorithm. However, after relaxation and canceling the integer constraint in (35e), $\mathcal{P}3 - 1$ can also be transformed into a convex problem as:

$$\mathcal{P}3 - 2 : \min_{\{K,z\}} z \tag{44a}$$

$$\text{s.t. Constraints (43b), (34b), (35d),} \tag{44b}$$

$$K_i > 0, \forall i \in [0, r-1], \tag{44c}$$

and optimal solution is given in Proposition 2 according to the KKT conditions.

Proposition 2. For given (N, K, L, d, r, μ, a) , the closed-form expression of the optimal solution $K^{[Prop2]}$ to $\mathcal{P}3 - 2$ is

$$\sum_{i=0}^{r-1} \frac{i+1}{z^* - a(i+1)} = \mu[rN - d(K + rL - r)], \tag{45a}$$

$$K_i^{[Prop2]} = \frac{N}{d} - \frac{i+1}{d\mu[z^* - a(i+1)]} - L + 1. \tag{45b}$$

Consequently, the MVD algorithm is used again to solve $\mathcal{P}3 - 1$ with a computational complexity of $O\left(\frac{Nr}{d}\right)$, and the rounded result of $K^{[Prop2]}$ is recommended to be used as the input.

6. Simulation Results

In this section, we leverage simulation results to evaluate the performance of APCC in terms of task completion delay and compare it with other state-of-the-art coded computing strategies, including LCC [15], LCC with multi-message communications (LCC-MMC) [35], and BACC [27]. Additionally, we analyze the impact of the number of partitioned sets r and the number of colluding workers L on the task completion delay of APCC.

In simulations, the entire task is given, leading to a constant computation load for the entire task. In this scenario, we aim to compare the entire task completion delay across various task divisions and coded computing strategies, illustrating the delay performance improvements introduced by APCC. We assume that the computation delay T_0 of a single worker to complete the entire task follows a shifted exponential distribution, which is modeled as:

$$\mathbb{P}[T_0 \leq t] = \begin{cases} 1 - e^{-\mu_0(t-a_0)}, & \text{if } t \geq a_0, \\ 0 & \text{otherwise,} \end{cases} \quad (46)$$

then the computation delay T of a single worker to complete one subtask follows:

$$\mathbb{P}[T \leq t] = \begin{cases} 1 - e^{-\mu_0(Kt-a_0)}, & \text{if } t \geq \frac{a_0}{K}, \\ 0 & \text{otherwise,} \end{cases} \quad (47)$$

where K denotes the task division number, which may vary depending on the chosen coded computing strategies. The parameter a_0 is set to 0.5 s, and μ_0 is set as $\frac{1}{10a_0}$. In APCC, $\{K_i\}_{i=0}^{r-1}$ corresponds to the number of subtasks in each set before encoding, and their values are obtained using the MVD algorithm. Then, 5×10^4 Monte Carlo realizations are run to obtain the average completion delay of the entire task, and the simulation codes are shared here (code link: <https://github.com/Zemiser/APCC>, accessed on 24 August 2024). Note that by comparing (47) with (31), we have $\mu = K\mu_0$ and $a = \frac{a_0}{K}$, and can further derive the distribution of T_m in (36).

The benchmarks involved in this section are as follows:

(1) *APCC*: APCC is our proposed coded computing strategy in this paper. It first divides the entire task into K subtasks and then partitions them into r sets with different sizes. The number of subtasks in set $i, i \in [0, r-1]$ is denoted as K_i , which satisfies $\sum_{i=0}^{r-1} K_i = K$. After that, each set is encoded into N subtasks assigned to the N workers. Consequently, each worker is assigned r subtasks. For Case 1 of APCC, the set i is recovered when the master has received $d(K_i + L - 1) + 1$ results, and the entire task is completed when all sets are recovered.

(2) *LCC*: LCC proposed in [15] divides the entire task into K' subtasks and then encodes them into N subtasks assigned to N workers. Each worker in LCC is assigned one subtask. Therefore, the entire task is completed when the master has received $d(K' + L - 1) + 1$ results. $L = 0$ means the absence of a requirement for privacy preservation. We assume that the number of workers N is greater than $dK' - 1$ to facilitate our analysis. Consequently, when $L = 0$, the recovery threshold is defined as $d(K' - 1) + 1$ instead of $N - \lfloor \frac{N}{K'} \rfloor + 1$ according to [15].

(3) *LCC-MMC*: MMC proposed in [35] is another approach to utilize the computing results of straggling workers except for the hierarchical structure. It also achieves a partial return of results from workers through a more granular task division. Specifically, LCC-MMC divides the entire task into K^{LM} subtasks and then encodes them into Nr subtasks. Each worker in LCC-MMC is assigned r subtasks and the entire task is completed when the master has received $d(K^{LM} - 1) + 1$ results. However, LCC-MMC cannot preserve the privacy of input data because multiple encoded data from the same encoding function are sent to a worker, which is different from the case of APCC where r subtasks assigned to the same worker are generated by r different encoding functions $\{g_i(x)\}_{i=0}^{r-1}$.

(4) *BACC*: The BACC strategy, as introduced in [27], offers approximated results with improved precision achievable by increasing the number of return results from workers. It shares a task division structure identical to LCC, partitioning the task into K' subtasks and then further encoding them into N subtasks. Each worker in BACC is assigned one such subtask.

To ensure fairness, all strategies employ an identical number of workers and distribute an equivalent computation load for a single worker. Assuming that the computation loads

of the entire task are $O(\gamma)$, then each subtask $f(\mathbf{D}_k)$ in APCC has a computation load of $O(\frac{\gamma}{K})$, and the computation loads of each worker in APCC are $O(\frac{\gamma^r}{K})$ because there are r partitioned sets. Similarly, we can derive that the computation loads of each worker in LCC, BACC and LCC-MMC are $O(\frac{\gamma}{K^r})$, $O(\frac{\gamma}{K^r})$ and $O(\frac{\gamma^r}{K^{LM}})$, respectively. In order to ensure that each worker in these schemes performs an identical fraction of the entire task as APCC, we have

$$K' = \frac{K^{LM}}{r} = \frac{K}{r}. \tag{48}$$

Due to the different applicability of various coded computing strategies, we will first conduct a comprehensive analysis and comparison of APCC alongside other strategies within the following three scenarios: (1) Accurate results with L colluding workers ($L > 0$); (2) Accurate results without colluding workers ($L = 0$); (3) Approximated results. Finally, we study the impact of the parameters r and L on the delay performance of APCC.

6.1. Accurate Results with L Colluding Workers ($L > 0$)

In this scenario, we consider the following three benchmarks: LCC, APCC without cancellation, and APCC with cancellation. For fair comparison, the computation load of workers should be set the same, so we have $K' = \frac{K}{r}$.

As shown in Figure 5, the average completion delay of the entire task $\{f(\mathbf{D}_k)\}_{k=0}^{K-1}$ first decreases and then increases with the task division number K , indicating the existence of an optimal division that minimizes the delay. This trade-off arises from balancing the computation load of each worker and the minimum number of workers needed to recover $\{f(\mathbf{D}_k)\}_{k=0}^{K-1}$. On the one hand, as the division number decreases, the computation load of each subtask increases, which leads to longer computation delays for each worker due to the increased workload. Although the number of workers waiting for results decreases, the increase in load negates this advantage. On the other hand, while the division number approaches the maximum, as illustrated in the inequality (24), the number of workers that the master needs to wait for approaches N , making the straggling effect a bottleneck for performance and increasing the delay. The zigzag fluctuations in the curve are mainly due to the integer values of the partitioning numbers.

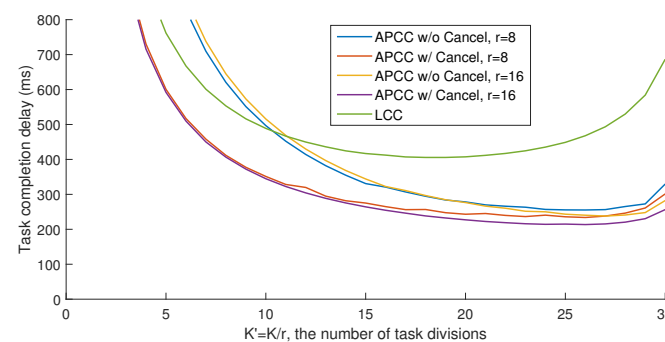


Figure 5. Delay performance comparison between APCC and LCC for accurate results with L colluding workers ($L > 0$). Settings: $N = 200, L = 20, d = 4$. The partitioning strategy $\{K_i\}$ of APCC is obtained by the proposed MVD algorithm. r is the number of partitioned sets.

Note that the primary metric for evaluating different schemes in our study is the minimum task completion delay under different division numbers, as depicted in Figure 5. This is because the division number $K' = \frac{K}{r}$ corresponds to the division of computation function inputs, which is typically a high-dimensional matrix. As such, K' can be adjusted flexibly in most cases. Therefore, the minimum achieved task completion delay is the main focus of our analysis.

Figure 6 compares APCC and LCC in terms of the minimum task completion delay. In these benchmarks, ‘Brute-Force’ refers to a partitioning strategy derived from an exhaustive

search across all possible values of $\{K_i\}$. Due to the highly complex traversal search, the brute-force results are only provided for scenarios with a smaller number of sets ($r = 4$). Figure 6 illustrates that both APCC with and without cancellation yield sufficient reductions in task completion delay compared to LCC. For instance, when $N = 100, L = 10, d = 2, r = 16$, and the partitioning strategy obtained from the MVD algorithm is utilized, APCC with and without cancellation achieve delay reductions of 41.4% and 47.5%, respectively, compared to LCC. Moreover, the comparison with the ‘Brute-Force’ benchmarks shows that the partitioning strategy $\{K_i\}$ obtained through the MVD algorithm is near-optimal.

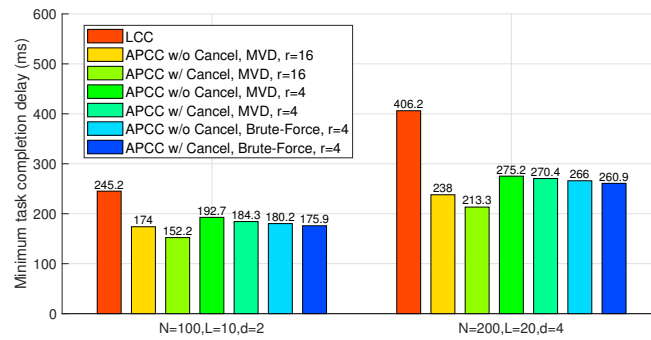


Figure 6. APCC vs. LCC. Minimum task completion delay achieved by all possible task divisions $K' = \frac{K}{r}$, applied to accurate results with L colluding workers ($L > 0$).

6.2. Accurate Results without Colluding Workers ($L = 0$)

In this scenario, we evaluate four benchmarks: LCC, LCC-MMC, and APCC with and without cancellation. Among these, only LCC does not consider partial results from straggling workers. Similar to Subsection IV.A, we set $K' = \frac{K^{LM}}{r} = \frac{K}{r}$, with K^{LM} representing the task division number for LCC-MMC.

In Figure 7, both LCC-MMC and APCC effectively reduce task completion delay compared to LCC. Specifically, when r is large enough, APCC with cancellation closely approaches the performance of LCC-MMC. This similarity arises because, in both APCC and LCC-MMC, the master utilizes nearly all computing results from workers when divided subtasks are sufficiently small. Figure 7 also illustrates that when privacy is not a concern, MMC is a viable method to reduce the delay in coded computing.

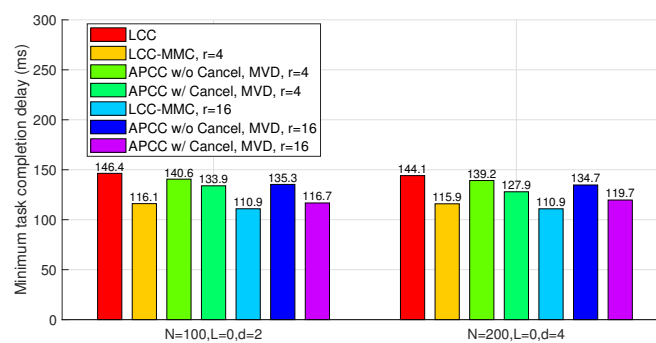


Figure 7. APCC vs. LCC and LCC-MMC. Minimum task completion delay achieved by all possible task divisions $K' = \frac{K^{LM}}{r} = \frac{K}{r}$, applied to accurate results without colluding workers ($L = 0$).

Compared to Figure 6, we observe that the absence of colluding workers limits the potential for delay optimization. For instance, with parameters $N = 100, L = 0, d = 2$, and $r = 16$, APCC with cancellation achieves only a 20.3% delay reduction compared to LCC.

6.3. Approximated Results

In this subsection, we compare the task completion delay of BACC and case 2 of APCC, which can both provide approximated results with fewer workers than the recovery

threshold. To ensure uniform worker computation load, we also set $K' = \frac{K}{r}$, as in our previous analysis. Furthermore, since BACC shares an identical task division structure with LCC, we employ a smaller recovery threshold of the same form as LCC to evaluate its delay performance. For instance, when the recovery threshold $d(K' + L - 1) + 1$ exceeds N , a reduced uniform recovery threshold $\frac{d}{2}(K' + L - 1) + 1$ below N can be employed for both BACC and APCC.

As shown in Figure 8, the hierarchical task partitioning and the cancellation of completed sets in APCC yield sufficient delay performance improvement. Compared to BACC, the proposed MVD algorithm for APCC achieves up to 42.9% delay reduction. Note that in this scenario, both APCC and BACC can obtain approximated results with fewer returned results, while LCC for accurate computation fails to work when K' is larger than 20 in the two cases of Figure 8, as the recovery threshold of LCC needs to be larger than $d(K' + L - 1) + 1$.

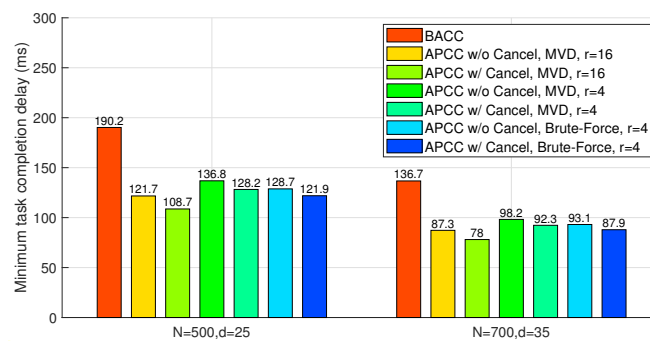


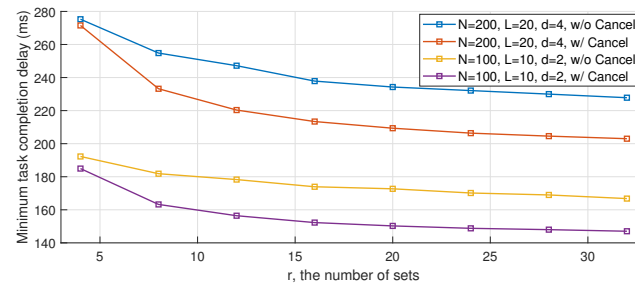
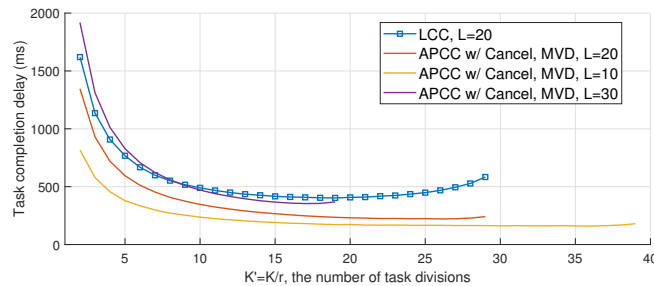
Figure 8. APCC vs. BACC. Minimum task completion delay achieved by all possible task divisions $K' = \frac{K}{r}$, applied to approximated results.

6.4. Impact of r and L on the Performance of APCC

The impact of the hierarchical partitioning number of sets r on the task completion delay of APCC is illustrated in Figure 9a. It is observed that a larger number of sets r results in a smaller computation delay, which is consistent with the results shown in previous figures. The reduction in delay can be attributed to the fact that a larger r implies a smaller computation load for each subtask in the hierarchical structure, and the difference in computation load between fast and slow workers can be described more precisely. Consequently, the proposed MVD algorithm can better utilize the computing results of straggling workers to reduce delay. Furthermore, Figure 9a indicates that the benefit of increasing r has a boundary effect, which corresponds to the upper bound of benefit brought by the granularity refinement of task divisions.

Recall that L denotes the maximum number of colluding workers that a coded computing scheme can tolerate. The value of L can serve as an indirect indicator of the level of privacy preservation offered by the scheme. Specifically, a larger value of L corresponds to more stringent privacy protection and a higher tolerance for colluders. It is demonstrated in Section 4.2 that complete data privacy can be achieved as long as the number of colluders remains below L .

Figure 9b illustrates the impact of the number of colluding workers L on the trade-off between delay and privacy preservation. It is worth noting that, for a fixed K' , increasing the value of L leads to a larger recovery threshold H for the original subtasks, which results in a longer task completion delay. Moreover, as demonstrated in (24), choosing a larger value of L restricts the maximum number of task divisions. Consequently, the range of K' values corresponding to the plotted curves in Figure 9b varies with L .

(a) Delay of APCC vs. r (b) $N = 200, d = 4, r = 12$ **Figure 9.** Delay performance of APCC with different r and L .

7. Conclusions

In this paper, we have investigated a distributed computing system that consists of one master and multiple workers. We have first proposed an adaptive privacy-preserving coded computing (APCC) strategy, which is suitable for diverse task scenarios and computation functions. APCC adaptively provides accurate or approximated results with controllable error according to the form of computation functions, and the computation process remains numerically stable. We have rigorously proved the optimality of APCC in terms of encoding rate based on the optimal recovery threshold of LCC. The complete privacy preservation of input data has also been proved.

We have further provided a low-complexity maximum value descent algorithm to optimally solve the hierarchical task partitioning problem in APCC, with and without considering cancellation, aiming at minimizing task completion delay. The cancellation is our proposed operation aiming to further accelerate computation by timely canceling the completed tasks. Extensive simulations have demonstrated that APCC outperforms the state-of-the-art coded computing strategies by a range of 20.3% to 42.9% in terms of task completion delay.

Author Contributions: Conceptualization, Q.Z. and S.Z.; Methodology, Q.Z. and Z.N.; Software, Q.Z.; Validation, Z.N.; Formal analysis, Z.N.; Resources, S.Z.; Writing—original draft, Q.Z.; Writing—review & editing, S.Z.; Project administration, S.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China under Grants 62341108; in part by the China Postdoctoral Science Foundation under Grant 2023M742011; and in part by the Fundamental Research Funds for the Central Universities under Grant 2242022k60006.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. Proof of the Inequality (23)

In this appendix, the proof for the optimal recovery threshold of LCC [15] to guarantee decodability is briefly introduced to enhance the clarity of the inequality (23). To achieve this, a weakened result under the condition of multilinearity is first derived. After that, in order to extend to the case of a general polynomial function, a construction of multilinear functions based on polynomial functions is provided.

The definition of the multilinear function is as follows:

Definition A1. For a multilinear function $f(D_1, D_2, \dots, D_d)$ with degree d , D_1, D_2, \dots, D_d are its d input variables, and f is linear with respect to each variable.

Under the assumption of the multilinearity of f , the optimal recovery threshold is provided in Lemma 1 of [15] as:

Lemma A1 ([15]). Consider an (N, S, L, f) coded computing problem, where N is the number of workers, S, L is the maximum number of stragglers and colluding workers that can be tolerated, respectively. f is a multilinear function, the degree of f is d , and the number of the equally divided input data is K . The optimal recovery threshold for linear coded computing schemes, denoted by H^* , is defined as:

$$H^* \triangleq \begin{cases} d(K + L - 1) + 1, & \text{if } L > 0, \\ \min\{d(K - 1) + 1, N - \lfloor \frac{N}{K} \rfloor + 1\} & \text{if } L = 0. \end{cases} \quad (\text{A1})$$

In order to generalize to the case of polynomial functions, a construction method of multilinear functions is given in Lemma 4 of [15] as follows:

Lemma A2 ([15]). For a general polynomial function f of degree d , f' is a function constructed based on f and satisfies:

$$f'(D_1, D_2, \dots, D_d) = \sum_{\mathcal{T} \subseteq [1:d]} [(-1)^{|\mathcal{T}|} f(\sum_{k \in \mathcal{T}} D_k)]. \quad (\text{A2})$$

Then, f' is multilinear with respect to the d inputs. Here, \mathcal{T} is a subset of the set $[1 : d]$ and the degree of f' also equals d because it is a linear combination of f .

Based on the above two lemmas, Lemma A1 can be extended to the case of general polynomial [15]. Moreover, the actual number of results returned by workers equals $(N - S)$, which must be larger than the recovery threshold. Consequently, to guarantee the decodability for general polynomial coded computing, $N - S \geq H^*$ should hold, and thus the Formula (23) is derived.

References

1. Dean, J.; Corrado, G.; Monga, R.; Chen, K.; Devin, M.; Mao, M.; Ranzato, M.; Senior, A.; Tucker, P.; Yang, K.; et al. Large scale distributed deep networks. In Proceedings of the NIPS'12: Proceedings of the 25th International Conference on Neural Information Processing Systems, Lake Tahoe, NV, USA, 3–6 December 2012; Volume 1, p. 25.
2. Abadi, M.; Barham, P.; Chen, J.; Chen, Z.; Davis, A.; Dean, J.; Devin, M.; Ghemawat, S.; Irving, G.; Isard, M.; et al. TensorFlow: A System for Large-Scale Machine Learning. In Proceedings of the 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI 16), Savannah, GA, USA, 2–4 November 2016; pp. 265–283.
3. Nguyen, G.; Dlugolinsky, S.; Bobák, M.; Tran, V.; López García, Á.; Heredia, I.; Malík, P.; Hluchý, L. Machine learning and deep learning frameworks and libraries for large-scale data mining: A survey. *Artif. Intell. Rev.* **2019**, *52*, 77–124. [CrossRef]
4. Sun, Y.; Zhang, F.; Zhao, J.; Zhou, S.; Niu, Z.; Gündüz, D. Coded computation across shared heterogeneous workers with communication delay. *IEEE Trans. Signal Process.* **2022**, *70*, 3371–3385. [CrossRef]
5. Dean, J.; Barroso, L.A. The tail at scale. *Commun. ACM* **2013**, *56*, 74–80. [CrossRef]
6. Tandon, R.; Lei, Q.; Dimakis, A.G.; Karampatziakis, N. Gradient coding: Avoiding stragglers in distributed learning. In Proceedings of the 34th International Conference on Machine Learning, Sydney, NSW, Australia, 6–11 August 2017; pp. 3368–3376.

7. Lee, K.; Lam, M.; Pedarsani, R.; Papailiopoulos, D.; Ramchandran, K. Speeding Up Distributed Machine Learning Using Codes. *IEEE Trans. Inf. Theory* **2018**, *64*, 1514–1529. [[CrossRef](#)]
8. Li, S.; Maddah-Ali, M.A.; Yu, Q.; Avestimehr, A.S. A Fundamental Tradeoff Between Computation and Communication in Distributed Computing. *IEEE Trans. Inf. Theory* **2018**, *64*, 109–128. [[CrossRef](#)]
9. Yu, Q.; Maddah-Ali, M.A.; Avestimehr, A.S. Polynomial codes: An optimal design for high-dimensional coded matrix multiplication. In Proceedings of the NIPS'17: Proceedings of the 31st International Conference on Neural Information Processing Systems, Long Beach, CA, USA, 4–9 December 2017; p. 30.
10. Yu, Q.; Maddah-Ali, M.A.; Avestimehr, A.S. Straggler mitigation in distributed matrix multiplication: Fundamental limits and optimal coding. *IEEE Trans. Inf. Theory* **2020**, *66*, 1920–1933. [[CrossRef](#)]
11. Ferdinand, N.; Draper, S.C. Hierarchical coded computation. In Proceedings of the 2018 IEEE International Symposium on Information Theory, Vail, CO, USA, 17–22 June 2018; pp. 1620–1624.
12. Reisizadeh, A.; Prakash, S.; Pedarsani, R.; Avestimehr, A.S. Coded computation over heterogeneous clusters. *IEEE Trans. Inf. Theory* **2019**, *65*, 4227–4242. [[CrossRef](#)]
13. Raghupathi, W.; Raghupathi, V. Big data analytics in healthcare: Promise and potential. *Health Inf. Sci. Syst.* **2014**, *2*, 1–10. [[CrossRef](#)]
14. McAfee, A.; Brynjolfsson, E.; Davenport, T.H.; Patil, D.; Barton, D. Big data: The management revolution. *Harv. Bus. Rev.* **2012**, *90*, 60–68.
15. Yu, Q.; Li, S.; Raviv, N.; Kalan, S.M.M.; Soltanolkotabi, M.; Avestimehr, S.A. Lagrange coded computing: Optimal design for resiliency, security, and privacy. In Proceedings of the 22nd International Conference on Artificial Intelligence and Statistics, AISTATS 2019, Naha, Japan, 16–18 April 2019; pp. 1215–1225.
16. Yang, H.; Lee, J. Secure Distributed Computing With Straggling Servers Using Polynomial Codes. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 141–150. [[CrossRef](#)]
17. Chang, W.T.; Tandon, R. On the capacity of secure distributed matrix multiplication. In Proceedings of the 2018 IEEE Global Communications Conference, Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6.
18. Aliasgari, M.; Simeone, O.; Kliever, J. Private and secure distributed matrix multiplication with flexible communication load. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2722–2734. [[CrossRef](#)]
19. Kim, M.; Lee, J. Private secure coded computation. In Proceedings of the 2019 IEEE International Symposium on Information Theory (ISIT), Paris, France, 7–12 July 2019; pp. 1097–1101.
20. Kakar, J.; Ebadifar, S.; Sezgin, A. On the capacity and straggler-robustness of distributed secure matrix multiplication. *IEEE Access* **2019**, *7*, 45783–45799. [[CrossRef](#)]
21. Nodehi, H.A.; Najarkolaei, S.R.H.; Maddah-Ali, M.A. Entangled polynomial coding in limited-sharing multi-party computation. In Proceedings of the 2018 IEEE Information Theory Workshop (ITW), Guangzhou, China, 25–29 November 2018; pp. 1–5.
22. Yu, Q.; Avestimehr, A.S. Entangled polynomial codes for secure, private, and batch distributed matrix multiplication: Breaking the “cubic” barrier. In Proceedings of the 2020 IEEE International Symposium on Information Theory (ISIT), Los Angeles, CA, USA, 21–26 June 2020; pp. 245–250.
23. Chang, W.T.; Tandon, R. On the upload versus download cost for secure and private matrix multiplication. In Proceedings of the 2019 IEEE Information Theory Workshop (ITW), Visby, Sweden, 25–28 August 2019; pp. 1–5.
24. D'Oliveira, R.G.; El Rouayheb, S.; Karpuk, D. GASP codes for secure distributed matrix multiplication. *IEEE Trans. Inf. Theory* **2020**, *66*, 4038–4050. [[CrossRef](#)]
25. Akbari-Nodehi, H.; Maddah-Ali, M.A. Secure Coded Multi-Party Computation for Massive Matrix Operations. *IEEE Trans. Inf. Theory* **2021**, *67*, 2379–2398. [[CrossRef](#)]
26. Tahmasebi, B.; Maddah-Ali, M.A. Private Function Computation. In Proceedings of the 2020 IEEE International Symposium on Information Theory (ISIT), Los Angeles, CA, USA, 21–26 June 2020; pp. 1118–1123.
27. Jahani-Nezhad, T.; Maddah-Ali, M.A. Berrut Approximated Coded Computing: Straggler Resistance Beyond Polynomial Computing. *IEEE Trans. Pattern Anal. Mach. Intell.* **2023**, *45*, 111–122. [[CrossRef](#)]
28. Jahani-Nezhad, T.; Maddah-Ali, M.A. CodedSketch: A coding scheme for distributed computation of approximated matrix multiplication. *IEEE Trans. Inf. Theory* **2021**, *67*, 4185–4196. [[CrossRef](#)]
29. Soleymani, M.; Ali, R.E.; Mahdavi, H.; Avestimehr, A.S. ApproxIFER: A model-agnostic approach to resilient and robust prediction serving systems. In Proceedings of the Thirty-Sixth AAAI Conference on Artificial Intelligence, AAAI 2022, Virtual Event, 22 February–1 March 2022; Volume 36, pp. 8342–8350.
30. Fahim, M.; Cadambe, V.R. Numerically stable polynomially coded computing. *IEEE Trans. Inf. Theory* **2021**, *67*, 2758–2785. [[CrossRef](#)]
31. Ramamoorthy, A.; Tang, L. Numerically Stable Coded Matrix Computations via Circulant and Rotation Matrix Embeddings. *IEEE Trans. Inf. Theory* **2022**, *68*, 2684–2703. [[CrossRef](#)]
32. Charalambides, N.; Mahdavi, H.; Hero, A.O. Numerically stable binary gradient coding. In Proceedings of the 2020 IEEE International Symposium on Information Theory, Los Angeles, CA, USA, 21–26 June 2020; pp. 2622–2627.
33. Buyukates, B.; Ulukus, S. Timely distributed computation with stragglers. *IEEE Trans. Commun.* **2020**, *68*, 5273–5282. [[CrossRef](#)]
34. Hasircioğlu, B.; Gómez-Vilardebó, J.; Gündüz, D. Bivariate polynomial coding for efficient distributed matrix multiplication. *IEEE J. Sel. Areas Inf. Theory* **2021**, *2*, 814–829. [[CrossRef](#)]

35. Ozfatura, E.; Ulukus, S.; Gündüz, D. Straggler-aware distributed learning: Communication–computation latency trade-off. *Entropy* **2020**, *22*, 544. [[CrossRef](#)] [[PubMed](#)]
36. Dutta, S.; Fahim, M.; Haddadpour, F.; Jeong, H.; Cadambe, V.; Grover, P. On the Optimal Recovery Threshold of Coded Matrix Multiplication. *IEEE Trans. Inf. Theory* **2020**, *66*, 278–301. [[CrossRef](#)]
37. Yang, C.S.; Avestimehr, A.S. Coded computing for secure Boolean computations. *IEEE J. Sel. Areas Inf. Theory* **2021**, *2*, 326–337. [[CrossRef](#)]
38. Tang, T.; Ali, R.E.; Hashemi, H.; Gangwani, T.; Avestimehr, S.; Annavaram, M. Adaptive verifiable coded computing: Towards fast, secure and private distributed machine learning. In Proceedings of the 2022 IEEE International Parallel and Distributed Processing Symposium (IPDPS), Lyon, France, 30 May–3 June 2022; pp. 628–638.
39. Soleymani, M.; Ali, R.E.; Mahdavi, H.; Avestimehr, A.S. List-decodable coded computing: Breaking the adversarial toleration barrier. *IEEE J. Sel. Areas Inf. Theory* **2021**, *2*, 867–878. [[CrossRef](#)]
40. Zhang, F.; Sun, Y.; Zhou, S. Coded computation over heterogeneous workers with random task arrivals. *IEEE Commun. Lett.* **2021**, *25*, 2338–2342. [[CrossRef](#)]
41. Wu, F.; Chen, L. Latency optimization for coded computation straggled by wireless transmission. *IEEE Wirel. Commun. Lett.* **2020**, *9*, 1124–1128. [[CrossRef](#)]
42. Van Huynh, N.; Hoang, D.T.; Nguyen, D.N.; Dutkiewicz, E. Joint Coding and Scheduling Optimization for Distributed Learning Over Wireless Edge Networks. *IEEE J. Sel. Areas Commun.* **2022**, *40*, 484–498. [[CrossRef](#)]
43. Kim, D.; Park, H.; Choi, J.K. Optimal Load Allocation for Coded Distributed Computation in Heterogeneous Clusters. *IEEE Trans. Commun.* **2021**, *69*, 44–58. [[CrossRef](#)]
44. Berrut, J.P.; Trefethen, L.N. Barycentric lagrange interpolation. *SIAM Rev.* **2004**, *46*, 501–517. [[CrossRef](#)]
45. Berrut, J.P. Rational functions for guaranteed and experimentally well-conditioned global interpolation. *Comput. Math. Appl.* **1988**, *15*, 1–16. [[CrossRef](#)]
46. Zeng, Q.; Zhou, S. On the Capacity of Privacy-Preserving and Straggler-Robust Distributed Coded Computing. In Proceedings of the 2021 IEEE/CIC International Conference on Communications in China (ICCC), Xiamen, China, 28–30 July 2021; pp. 664–669.
47. Lawler, E.L.; Wood, D.E. Branch-and-bound methods: A survey. *Oper. Res.* **1966**, *14*, 699–719. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.