

A Systematic Approach towards Efficient Private Matrix Multiplication

Jinbao Zhu and Songze Li

Abstract—We consider the problems of Private and Secure Matrix Multiplication (PSMM) and Fully Private Matrix Multiplication (FPMM), for which matrices privately selected by a master node are multiplied at distributed worker nodes without revealing the indices of the selected matrices, even when a certain number of workers collude with each other. We propose a novel systematic approach to solve PSMM and FPMM with colluding workers, which leverages solutions to a related Secure Matrix Multiplication (SMM) problem where the data (rather than the indices) of the multiplied matrices are kept private from colluding workers. Specifically, given an SMM strategy based on polynomial codes or Lagrange codes, one can exploit the special structure inspired by the matrix encoding function to design private coded queries for PSMM/FPMM, such that the algebraic structure of the computation result at each worker resembles that of the underlying SMM strategy. Adopting this systematic approach provides novel insights in private query designs for private matrix multiplication, substantially simplifying the processes of designing PSMM and FPMM strategies. Furthermore, the PSMM and FPMM strategies constructed following the proposed approach outperform the state-of-the-art strategies in one or more performance metrics including recovery threshold (minimal number of workers the master needs to wait for before correctly recovering the multiplication result), communication cost, and computation complexity, demonstrating a more flexible tradeoff in optimizing system efficiency.

Index Terms—Coded distributed computing, secure matrix multiplication, private and secure matrix multiplication, fully private matrix multiplication, polynomial codes, Lagrange codes.

I. INTRODUCTION

IN the era of Big Data, performing computationally intensive tasks on a single machine is becoming infeasible due to limited processing power and storage space. As an efficient solution, distributed computing has emerged as a natural approach to overcome such limitations, by partitioning the large computing task into smaller sub-tasks, and outsourcing them to many distributed worker nodes. However, scaling out the computation across distributed workers is also faced with efficiency challenges including additional communication overhead compared to centralized processing, and prolonged task execution time due to slow or delay-prone worker nodes,

known as the *straggler effect* [1], [2]. Meanwhile, distributing sensitive raw data across worker nodes may raise serious security and privacy concerns. Therefore, designing computation and communication efficient strategies that are robust to straggler effect, while providing data privacy and security is of vital importance for distributed computing applications.

Matrix multiplication, as one of the key building blocks in various engineering applications like machine learning and big data analysis, is typically carried out in a distributed manner for practically sized input matrices [3]–[6]. In this paper we focus on improving the computation and communication efficiency of two distributed private matrix multiplication problems, over a distributed computing system consisting of a master node and N worker nodes. For the first *Private and Secure Matrix Multiplication* (PSMM) problem, as illustrated in Fig. 1, the master owns a confidential matrix \mathbf{A} and all workers have access to a library \mathcal{L}^B of V public matrices $\mathbf{B}^{(1)}, \mathbf{B}^{(2)}, \dots, \mathbf{B}^{(V)}$. The goal of the master is to compute the product $\mathbf{A}\mathbf{B}^{(\theta)}$ for some $\theta \in \{1, 2, \dots, V\}$ from the distributed system, while keeping the index θ private and the matrix \mathbf{A} secure from any up to T colluding workers.

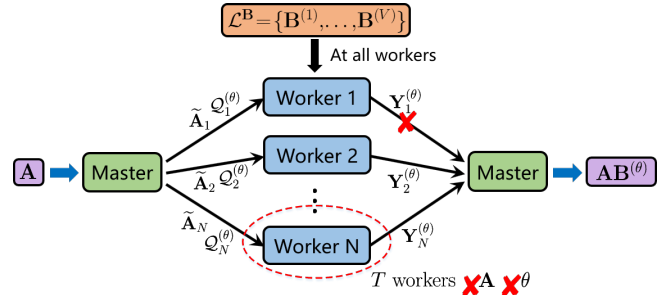


Fig. 1. System model for private and secure matrix multiplication. The master sends a coded matrix $\tilde{\mathbf{A}}_i$ and a query $Q_i^{(\theta)}$ to worker i with the private index θ . Each worker i uses $\tilde{\mathbf{A}}_i$, $Q_i^{(\theta)}$, and the public library \mathcal{L}^B to compute a response $\mathbf{Y}_i^{(\theta)}$. The master must be able to decode the product $\mathbf{A}\mathbf{B}^{(\theta)}$ from the responses of servers in the presence of stragglers.

To do that, the master sends an encoded version of the matrix \mathbf{A} to each worker, along with a query that instructs the worker to encode the library \mathcal{L}^B and compute a response for the master. To mitigate the influence of stragglers, the master only waits for the responses from a subset of fastest workers to recover the desired product $\mathbf{A}\mathbf{B}^{(\theta)}$, where the minimum number of successful computing workers that the master needs to wait for is referred to as *recovery threshold*. In the second problem of interest shown in Fig. 2, referred to as *Fully Private Matrix Multiplication* (FPMM), the matrix \mathbf{A} is selected from another public library \mathcal{L}^A of U matrices $\mathbf{A}^{(1)}, \mathbf{A}^{(2)}, \dots, \mathbf{A}^{(U)}$

This work was supported in part by the National Nature Science Foundation of China (NSFC) under Grant 62106057.

Jinbao Zhu is with the Thrust of Internet of Things, The Hong Kong University of Science and Technology (Guangzhou), Guangzhou 510006, China (e-mail: jbzhu@ust.hk).

Songze Li is with the Thrust of Internet of Things, The Hong Kong University of Science and Technology (Guangzhou), Guangzhou 510006, China, and also with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Hong Kong SAR, China (e-mail: songzeli@ust.hk).

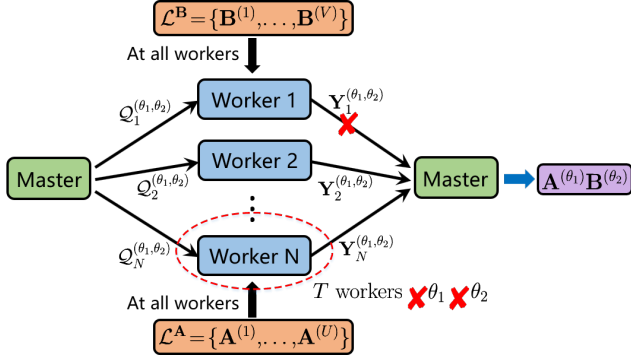


Fig. 2. System model for fully private matrix multiplication. The master sends a query $Q_i^{(\theta_1, \theta_2)}$ to worker i with the private indices θ_1 and θ_2 . Each worker i uses $Q_i^{(\theta_1, \theta_2)}$, and the public libraries \mathcal{L}^A and \mathcal{L}^B to compute a response $Y_i^{(\theta)}$. The master must be able to decode the product $A^{(\theta_1)}B^{(\theta_2)}$ from the responses of servers in the presence of stragglers.

that are shared by all workers along with the library \mathcal{L}^B . In this case, the master wishes to compute $A^{(\theta_1)}B^{(\theta_2)}$ for some $\theta_1 \in \{1, 2, \dots, U\}$ and $\theta_2 \in \{1, 2, \dots, V\}$, without revealing any information about the indices θ_1 and θ_2 to any T colluding workers. Private matrix multiplication [7], [8] has a wide range of application scenarios in practice. For instance, consider a recommender system based on collaborative filtering, where recommendations are generated by computing the product of two matrices, one describing the profiles of the users, and another one representing the profiles of the items. Given that the user profile matrix may reveal the users' private information, and the queried user and item indices may leak the privacy of the recommendation requester, data security and query privacy should be provided by the recommendation service.

Secure Matrix Multiplication (SMM) is another problem that is related to the interested PSMM and FPMM problems. In SMM, the master wishes to compute the product of two owned matrices \mathbf{A} and \mathbf{B} in the distributed system, without revealing anything about \mathbf{A} and \mathbf{B} to the workers. Computing strategies for the SMM problem, based on how the matrices \mathbf{A} and \mathbf{B} are securely encoded, can be categorised into SMM based on polynomial codes [7], [9]–[15] and SMM based on Lagrange codes [16], [17], where polynomial codes [18]–[21] and Lagrange codes [22] are constructed by leveraging the algebraic structure of polynomial functions and Lagrange interpolate polynomials, respectively. An essential component behind these coded strategies is to construct appropriate encoding functions of \mathbf{A} and \mathbf{B} , such that the desired product \mathbf{AB} can be recovered by interpolating a polynomial from worker responses. The state-of-the-art strategies for SMM based on polynomial codes and Lagrange codes are reflected in [11], [15] and [16], respectively. Having observed the similarities between PSMM/FPMM and SMM in requiring privacy-preserving matrix multiplication, and their key difference that whether or not queries for the workers are needed, we are interested in the question:

Would it be possible to construct an efficient PSMM/FPMM strategy, simply via designing private queries on top of an SMM strategy?

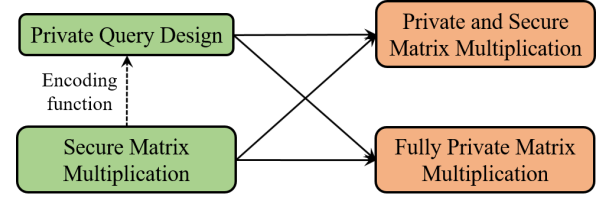


Fig. 3. Illustration of the proposed approach to design PSMM and FPMM solutions from a SMM solution and a compatible private query design.

We answer the above question in the affirmative, and propose a novel systematic approach to construct efficient computation strategies for both PSMM and FPMM problems. Specifically, as illustrated in Fig. 3, we start with an SMM strategy (based on polynomial codes or Lagrange codes), and make use of the special structure inspired by the matrix encoding functions in the SMM strategy to create private queries that facilitate a form of interference alignment, separating the desired and interfering partitions of the matrices in the libraries, such that the response computed at each worker has identical structure as that of the SMM strategy. Consequently, as in the SMM strategy, the desired product can be recovered via polynomial interpolation from the responses, with the same recovery threshold. Our major contributions in this paper are

- Establishes a generic connection between the PSMM/FPMM and the SMM problem, which helps to significantly simplify the design process of a PSMM/FPMM strategy;
- Compared with state-of-the-art PSMM and FPMM strategies, the strategies constructed from the proposed approach introduce new private query designs, and achieve more flexible tradeoffs between recovery threshold, communication cost and computation complexity, further improving the system efficiency. See Section VII for detailed comparisons.

A. Related Work

Coded computing has recently emerged as a technique of utilizing information/coding theoretical tools to inject redundant data and computations into distributed computing systems, to mitigate communication and straggler bottlenecks, and provide security and privacy for various computation tasks (see, e.g., [5], [10], [11], [15], [16], [19], [20], [22]–[33]). Privately retrieving a message from a distributed storage system without revealing the index of the message has been studied extensively in the problem of Private Information Retrieval (PIR) [34]–[40] in recent years. With the focus on index privacy, the PSMM and FPMM problems can be viewed as secure matrix multiplication problems with additional PIR requirement on the indices of interested matrices within public libraries.

Private and Secure Matrix Multiplication: The problem of private matrix multiplication was first introduced in [41] without colluding constraint (i.e., $T = 1$) and security guarantee on \mathbf{A} . The work [8] imposed the security constraint on \mathbf{A} to consider a non-colluding PSMM problem, and improved the recovery threshold of the strategy proposed in [41], through adopting the random query design in [35] to ensure privacy, and employing polynomial codes [18] to complete desired

computation. Subsequently in [30], the authors presented another non-colluding PSMM strategy that combines MDS-coded PIR scheme [38] with polynomial codes, and show that the strategy outperforms [8] in terms of upload and download communication costs. However, the strategy in [30] provides no resistance to stragglers, and has a high computation complexity. Further in [42], for the asymptotic setting (i.e., the number of matrices $V \rightarrow \infty$), a better tradeoff between upload and download cost was achieved by exploiting the idea of PIR based on Cross Subspace Alignment (CSA) [43], at the expense of a higher computation complexity. The authors proposed in [7], [44] novel strategies for the non-colluding PSMM problem using the query design in [8], yielding a more flexible tradeoff between recovery threshold, communication cost and computation complexity. Lagrange codes [22] were also employed to create non-colluding PSMM strategy [16], with the help of the query design in [8] and bilinear complexity [45], [46]. A very recent work [47] presented a computation strategy based on polynomial codes for the T -colluding PSMM problem considered in this paper, but it requires excessive communication cost and computation complexity.

Fully Private Matrix Multiplication: Much less work has been done in the literature for FPMM problem. In [16], a non-colluding FPMM strategy was proposed based on Lagrange codes and bilinear complexity, by resorting to the query design in [8]. Later in [48], a T -colluding FPMM strategy was introduced by using the idea of CSA.

In general, the current works [7], [16], [44] have well addressed the problems of PSMM and FPMM without colluding constraint. It is valuable to note that, all these works construct their strategies using the query design in [8] to ensure privacy, i.e., there is no difference in the private queries sent to workers. While the PSMM and FPMM problems with colluding constraint have been studied in [47], [48], these strategies require either high recovery threshold or huge communication cost and computation complexity.

B. Organization

The rest of this paper is organized as follows. In Section II, we formally formulate the problems of PSMM and FPMM. In Section III, we review the problem of SMM and its strategies based on polynomial codes and Lagrange codes. In Section IV, we summarize the main results of the paper. Sections V and VI present the proposed computation strategies for PSMM and FPMM, respectively, by exploiting the encoding structure of SMM strategies. Section VII gives comparison with other related work. Finally, the paper is concluded in Section VIII.

Notation: Let boldface and cursive capital letters represent matrices and sets, respectively, e.g., \mathbf{A} and \mathcal{K} . For a finite set \mathcal{K} , $|\mathcal{K}|$ denotes its cardinality. Denote \mathbb{Z}^+ the set of positive integers. For any $m, n \in \mathbb{Z}^+$ such that $m < n$, $[n]$ and $[m : n]$ denote the sets $\{1, 2, \dots, n\}$ and $\{m, m+1, \dots, n\}$, respectively. Define $A_{\mathcal{K}}$ as $\{A_{k_1}, \dots, A_{k_m}\}$ for any index set $\mathcal{K} = \{k_1, \dots, k_m\} \subseteq [n]$.

II. PROBLEM FORMULATIONS

Consider a distributed computing system consisting of one master node and N worker nodes, where each worker is connected to the master through an orthogonal communication link. The workers are honest-but-curious, which means that they will follow the prescribed protocol faithfully, yet may potentially collude to infer information about additional data inputs. We consider two private distributed matrix computation problems of *private and secure matrix multiplication* and *fully private matrix multiplication*. In the rest of this section, we describe the formulations of these two problems respectively.

A. Private and Secure Matrix Multiplication

For the problem of Private and Secure Matrix Multiplication (PSMM) depicted in Fig. 1, the master owns a *confidential* matrix \mathbf{A} of dimension $\lambda \times \omega$, and all workers have access to a library \mathcal{L}^B of V *public* matrices $\mathbf{B}^{(1)}, \mathbf{B}^{(2)}, \dots, \mathbf{B}^{(V)}$ with dimension $\omega \times \gamma$, for some $\lambda, \omega, \gamma \in \mathbb{Z}^+$. All the entries of the matrices are over a finite field \mathbb{F}_q for some prime power q .

The master privately selects an index $\theta \in [V]$ and wishes to compute the product $\mathbf{A}\mathbf{B}^{(\theta)}$ from the distributed system, while keeping its interested index θ private and its own matrix \mathbf{A} secure from any colluding subset of up to T out of the N workers. To this end, the master employs a computation strategy of PSMM consisting of the following three phases:

- **Sharing:** To ensure security, the master locally generates a private randomness, denoted by \mathcal{Z}^A , which is used to encode the matrix \mathbf{A} according to encoding functions $\mathbf{f} = (f_1, \dots, f_N)$, where f_i is the encoding function for worker i . Denote the encoded version of matrix \mathbf{A} for worker i by $\tilde{\mathbf{A}}_i$, i.e.,

$$\tilde{\mathbf{A}}_i = f_i(\mathbf{A}, \mathcal{Z}^A), \quad \forall i \in [N].$$

To privately complete computation, the master also generates N queries $\mathcal{Q}_{[N]}^{(\theta)}$ based on the index θ and another locally generated private randomness \mathcal{Z}^θ . Then the encoded matrix $\tilde{\mathbf{A}}_i$ and the query $\mathcal{Q}_i^{(\theta)}$ are shared with worker $i \in [N]$.

- **Computation:** Upon receiving $\mathcal{Q}_i^{(\theta)}$, worker i first uses encoding function h_i to encode the library \mathcal{L}^B into $\tilde{\mathbf{B}}_i$, i.e.,

$$\tilde{\mathbf{B}}_i = h_i(\mathbf{B}^{([V])}, \mathcal{Q}_i^{(\theta)}), \quad \forall i \in [N],$$

and then computes the response $\mathbf{Y}_i^{(\theta)}$ and sends it back to the master, which is a deterministic function of the received $\tilde{\mathbf{A}}_i$ and the encoded matrix $\tilde{\mathbf{B}}_i$.

- **Reconstruction:** For some design parameter $K \leq N$, the master only waits for the responses from the fastest K workers, and recovers the desired product $\mathbf{A}\mathbf{B}^{(\theta)}$ from their responses. This allows the computation strategy to tolerate any subset of up to $N - K$ stragglers.

A valid PSMM strategy must satisfy the following three requirements.

- **Privacy Constraint:** The strategies for computing any two distinct products $\mathbf{A}\mathbf{B}^{(\theta)}$ and $\mathbf{A}\mathbf{B}^{(\theta')}$ must be indis-

tinguishable with respect to any T colluding workers, i.e., for all $\theta \neq \theta' \in [V]$ and $\mathcal{T} \subseteq [N], |\mathcal{T}| = T$,

$$(\mathcal{Q}_{\mathcal{T}}^{(\theta)}, \tilde{\mathbf{A}}_{\mathcal{T}}, \mathbf{B}^{([V])}, \mathbf{Y}_{\mathcal{T}}^{(\theta)}) \sim (\mathcal{Q}_{\mathcal{T}}^{(\theta')}, \tilde{\mathbf{A}}_{\mathcal{T}}, \mathbf{B}^{([V])}, \mathbf{Y}_{\mathcal{T}}^{(\theta')}),$$

where $X \sim Y$ means that the random variables X and Y are identically distributed. Equivalently, the index θ of the desired product is hidden from all the information available to any T colluding workers, i.e.,

$$I(\theta; \mathcal{Q}_{\mathcal{T}}^{(\theta)}, \tilde{\mathbf{A}}_{\mathcal{T}}, \mathbf{B}^{([V])}, \mathbf{Y}_{\mathcal{T}}^{(\theta)}) = 0. \quad (1)$$

- **Security Constraint:** Any T colluding workers must not learn any information about the confidential matrix \mathbf{A} , i.e., for all $\mathcal{T} \subseteq [N], |\mathcal{T}| = T$,

$$I(\mathbf{A}; \mathcal{Q}_{\mathcal{T}}^{(\theta)}, \tilde{\mathbf{A}}_{\mathcal{T}}, \mathbf{B}^{([V])}, \mathbf{Y}_{\mathcal{T}}^{(\theta)}) = 0. \quad (2)$$

- **Correctness Constraint:** The desired product should be correctly reconstructed from the collection of responses of any fastest K workers, i.e.,

$$H(\mathbf{AB}^{(\theta)} | \mathbf{Y}_{\mathcal{K}}^{(\theta)}) = 0, \quad \forall \mathcal{K} \subseteq [N], |\mathcal{K}| = K.$$

The performance of a PSMM strategy is evaluated by the following key metrics:

1. The recovery threshold K , which is the minimum number of workers that the master needs to wait for in order to recover the desired product $\mathbf{AB}^{(\theta)}$.
2. The communication cost, which is comprised of the upload cost for matrix \mathbf{A} and download cost from workers,¹ defined as

$$P_u \triangleq \frac{\sum_{i=1}^N H(\tilde{\mathbf{A}}_i)}{\lambda \omega}, \quad P_d \triangleq \max_{\mathcal{K}: \mathcal{K} \subseteq [N], |\mathcal{K}| = K} \frac{H(\mathbf{Y}_{\mathcal{K}}^{(\theta)})}{\lambda \gamma}, \quad (3)$$

which are normalized with the number of symbols contained in the matrix \mathbf{A} and the desired product $\mathbf{AB}^{(\theta)}$, respectively.

3. The computation complexity, which includes the complexities of encoding, worker computation and decoding. The encoding complexity C_A at the master is defined as the number of arithmetic operations required to compute the encoding functions \mathbf{f} . The complexity of worker computation C_w is defined as the maximal number of arithmetic operations required to compute the response $\mathbf{Y}_i^{(\theta)}$, over all worker $i \in [N]$. Finally, the decoding complexity C_d at the master is defined as the maximal number of arithmetic operations required to decode the desired product $\mathbf{AB}^{(\theta)}$ from the responses of fastest workers in \mathcal{K} , over all $\mathcal{K} \subseteq [N]$ with $|\mathcal{K}| = K$.

B. Fully Private Matrix Multiplication

We describe the problem of Fully Private Matrix Multiplication (FPMM) illustrated in Fig. 2. In contrast to the above PSMM problem where the master has a confidential matrix \mathbf{A} , in the FPMM problem, there is a library \mathcal{L}^A of U public

matrices $\mathbf{A}^{(1)}, \mathbf{A}^{(2)}, \dots, \mathbf{A}^{(U)} \in \mathbb{F}_q^{\lambda \times \omega}$ that are accessible to the N workers, i.e., each worker has access to the two libraries \mathcal{L}^A and \mathcal{L}^B . The master is interested in computing the product $\mathbf{A}^{(\theta_1)} \mathbf{B}^{(\theta_2)}$ utilizing the distributed computing system, while keeping the indices of the desired product θ_1 and θ_2 private from any T colluding workers, for any $\theta_1 \in [U]$ and $\theta_2 \in [V]$.

To do so, similar to PSMM, a computation strategy for FPMM operates in the following three phases:

- **Sharing:** The master generates the queries $\mathcal{Q}_{[N]}^{(\theta_1)}$ and $\mathcal{Q}_{[N]}^{(\theta_2)}$ for the two libraries \mathcal{L}^A and \mathcal{L}^B according to the interested indices θ_1 and θ_2 and locally generated private randomness \mathcal{Z}^{θ_1} and \mathcal{Z}^{θ_2} respectively, and then shares $\mathcal{Q}_i^{(\theta_1)}$ and $\mathcal{Q}_i^{(\theta_2)}$ with worker $i \in [N]$.
- **Computation:** Upon receiving $\mathcal{Q}_i^{(\theta_1)}$ and $\mathcal{Q}_i^{(\theta_2)}$, worker i first encodes the two libraries \mathcal{L}^A and \mathcal{L}^B using encoding functions f_i and h_i , respectively. The encoded versions of \mathcal{L}^A and \mathcal{L}^B for worker $i \in [N]$ are given by

$$\tilde{\mathbf{A}}_i = f_i(\mathbf{A}^{([U])}, \mathcal{Q}_i^{(\theta_1)}), \quad \tilde{\mathbf{B}}_i = h_i(\mathbf{B}^{([V])}, \mathcal{Q}_i^{(\theta_2)}).$$

Then the worker i computes the response $\mathbf{Y}_i^{(\theta_1, \theta_2)}$ and sends it back to the master, which is a function of the encoded matrices $\tilde{\mathbf{A}}_i$ and $\tilde{\mathbf{B}}_i$.

- **Reconstruction:** The master recovers the desired product $\mathbf{A}^{(\theta_1)} \mathbf{B}^{(\theta_2)}$ from the responses of any fastest K workers.

A valid computation strategy for FPMM must satisfy the following constraints.

- **Fully Privacy Constraint:** The desired indices θ_1 and θ_2 must be hidden from all the information available to any T colluding workers, i.e., for all $\mathcal{T} \subseteq [N], |\mathcal{T}| = T$,

$$I(\theta_1, \theta_2; \mathcal{Q}_{\mathcal{T}}^{(\theta_1)}, \mathcal{Q}_{\mathcal{T}}^{(\theta_2)}, \mathbf{A}^{([U])}, \mathbf{B}^{([V])}, \mathbf{Y}_{\mathcal{T}}^{(\theta_1, \theta_2)}) = 0. \quad (4)$$

- **Correctness Constraint:** With the responses of any fastest K workers, the desired product must be recovered, i.e.,

$$H(\mathbf{A}^{(\theta_1)} \mathbf{B}^{(\theta_2)} | \mathbf{Y}_{\mathcal{K}}^{(\theta_1, \theta_2)}) = 0, \quad \forall \mathcal{K} \subseteq [N], |\mathcal{K}| = K.$$

Similar to the PSMM problem, the performance of an FPMM strategy is evaluated by the following key quantities: 1) the recovery threshold K ; 2) the normalized download cost P_d ; and 3) the computation complexities consisting of generating response at each worker C_w and decoding desired product at the master C_d .

For the above formulated PSMM and FPMM problems, our goal in this paper is to design efficient computation strategies that minimize the recovery threshold, the communication cost and the computation complexity. As the first step, we review the strategies proposed to solve a related distributed matrix multiplication problem, which serves as a building block of our approach to solve the private matrix multiplication problems.

III. PRELIMINARIES: SECURE MATRIX MULTIPLICATION

In this section, we summarize the state-of-the-art computation strategies for the Secure Matrix Multiplication (SMM) problem, which will be exploited to construct the strategies for PSMM and FPMM in the following sections. In the SMM problem, the master owns two confidential matrices

¹As in the information-theoretic PIR problem [36]–[40], the upload cost for queries can be neglected compared to the upload cost for matrix \mathbf{A} and the download cost, as it does not scale with matrix dimensions. Similarly, in the following, the computation complexity for queries are also neglected.

$\mathbf{A} \in \mathbb{F}_q^{\lambda \times \omega}$ and $\mathbf{B} \in \mathbb{F}_q^{\omega \times \gamma}$, and is interested in computing the product $\mathbf{C} = \mathbf{AB}$ in the distributed computing system, without revealing anything about \mathbf{A} and \mathbf{B} to any T colluding workers.

We first introduce a lemma that will be used in security and privacy proofs.

Lemma 1 (Generalized Secret Sharing [15], [49]). *For any parameters $L, T, \kappa, \tau \in \mathbb{Z}^+$, let $\mathbf{W}_1, \dots, \mathbf{W}_L \in \mathbb{F}_q^{\kappa \times \tau}$ be L secrets, and $\mathbf{Z}_1, \dots, \mathbf{Z}_T$ be T random matrices with the same dimensions as secrets whose entries are chosen independently and uniformly from \mathbb{F}_q . Let $\alpha_1, \dots, \alpha_N$ be N pairwise distinct elements from \mathbb{F}_q . Define a function of x as*

$$y(x) = \mathbf{W}_1 u_1(x) + \dots + \mathbf{W}_L u_L(x) + \mathbf{Z}_1 v_1(x) + \dots + \mathbf{Z}_T v_T(x),$$

where $u_1(x), \dots, u_L(x), v_1(x), \dots, v_T(x) \in \mathbb{F}_q[x]$ are the deterministic functions of x . If the matrix

$$\mathbf{V} = \begin{bmatrix} v_1(\alpha_{i_1}) & \dots & v_T(\alpha_{i_1}) \\ \vdots & \ddots & \vdots \\ v_1(\alpha_{i_T}) & \dots & v_T(\alpha_{i_T}) \end{bmatrix}_{T \times T}$$

is non-singular over \mathbb{F}_q for any $\mathcal{T} = \{i_1, \dots, i_T\} \subseteq [N]$ with $|\mathcal{T}| = T$, then the T values $y(\alpha_{i_1}), \dots, y(\alpha_{i_T})$ can not learn any information about the secrets $\mathbf{W}_1, \dots, \mathbf{W}_L$, i.e.,

$$I(y(\alpha_{i_1}), \dots, y(\alpha_{i_T}); \mathbf{W}_1, \dots, \mathbf{W}_L) = 0.$$

Let $m, p, n \in \mathbb{Z}^+$ be any partitioning parameters of data matrices such that $m|\lambda, p|\omega$ and $n|\gamma$. To efficiently exploit the computation power of distributed workers and establish the feasible tradeoff between system performance, the matrices \mathbf{A} and \mathbf{B} are partitioned into $m \times p$ and $p \times n$ equal-size sub-matrices, respectively, as shown below.

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_{1,1} & \dots & \mathbf{A}_{1,p} \\ \vdots & \ddots & \vdots \\ \mathbf{A}_{m,1} & \dots & \mathbf{A}_{m,p} \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} \mathbf{B}_{1,1} & \dots & \mathbf{B}_{1,n} \\ \vdots & \ddots & \vdots \\ \mathbf{B}_{p,1} & \dots & \mathbf{B}_{p,n} \end{bmatrix}, \quad (5)$$

where $\mathbf{A}_{k,\ell} \in \mathbb{F}_q^{\frac{\lambda}{m} \times \frac{\omega}{p}}$ for any $k \in [m], \ell \in [p]$ and $\mathbf{B}_{\ell,j} \in \mathbb{F}_q^{\frac{\omega}{p} \times \frac{\gamma}{n}}$ for any $\ell \in [p], j \in [n]$. Accordingly, the desired product $\mathbf{C} = \mathbf{AB}$ involves a total of mn linear combinations of products of sub-matrices, i.e.,

$$\mathbf{C} = \mathbf{AB} = \begin{bmatrix} \mathbf{C}_{1,1} & \dots & \mathbf{C}_{1,n} \\ \vdots & \ddots & \vdots \\ \mathbf{C}_{m,1} & \dots & \mathbf{C}_{m,n} \end{bmatrix}, \quad (6)$$

where $\mathbf{C}_{k,j} = \sum_{\ell=1}^p \mathbf{A}_{k,\ell} \mathbf{B}_{\ell,j}$ for all $k \in [m], j \in [n]$.

To the best of our knowledge, the state-of-the-art strategies for SMM with arbitrary partitioning of matrices above can be divided into two categories in terms of coding techniques, i.e., SMM based on polynomial codes [11], [15] and SMM based on Lagrange codes [16]. The essential components behind these coded strategies lie in constructing the encoding functions of matrices \mathbf{A} and \mathbf{B} , denoted by $f(x)$ and $h(x)$ respectively, such that the desired products of sub-matrices $\mathbf{C}_{k,j}, k \in [m], j \in [n]$ can be recovered by interpolating the product polynomial $g(x) = f(x) \cdot h(x)$. Next, we present these two approaches and their performance.

A. Secure Matrix Multiplication Based on Polynomial Codes

Let $\mathbf{Z}_1^{\mathbf{A}}, \dots, \mathbf{Z}_T^{\mathbf{A}}$ and $\mathbf{Z}_1^{\mathbf{B}}, \dots, \mathbf{Z}_T^{\mathbf{B}}$ be T random matrices distributed independently and uniformly on $\mathbb{F}_q^{\frac{\lambda}{m} \times \frac{\omega}{p}}$ and $\mathbb{F}_q^{\frac{\omega}{p} \times \frac{\gamma}{n}}$, respectively. In general, the goal of SMM strategies based on polynomial codes is to design a group of appropriate positive integers $\{a_{k,\ell}, b_{\ell,j}, c_t, d_t : k \in [m], \ell \in [p], j \in [n], t \in [T]\}$ to construct the encoding functions of matrices \mathbf{A} and \mathbf{B} (5) as

$$f_P(x) = \sum_{k=1}^m \sum_{\ell=1}^p \mathbf{A}_{k,\ell} x^{a_{k,\ell}} + \sum_{t=1}^T \mathbf{Z}_t^{\mathbf{A}} x^{c_t}, \quad (7)$$

$$h_P(x) = \sum_{\ell=1}^p \sum_{j=1}^n \mathbf{B}_{\ell,j} x^{b_{\ell,j}} + \sum_{t=1}^T \mathbf{Z}_t^{\mathbf{B}} x^{d_t}, \quad (8)$$

such that the following criteria are satisfied:

C1 The product polynomial

$$g(x) = \sum_{r=0}^{\delta} g_r x^r = f_P(x) \cdot h_P(x)$$

contains all the desired sub-products $\mathbf{C}_{k,j}, k \in [m], j \in [n]$ as coefficients, i.e., $\mathbf{C}_{k,j} \in \{g_r : r \in [0 : \delta]\}$ for all $k \in [m], j \in [n]$, where g_r is the coefficient of x^r in $f_P(x) \cdot h_P(x)$, and δ is the degree of the polynomial $f_P(x) \cdot h_P(x)$, given by

$$\delta \triangleq \max\{a_{k,\ell}, c_t : k \in [m], \ell \in [p], t \in [T]\} \\ + \max\{b_{\ell,j}, d_t : \ell \in [p], j \in [n], t \in [T]\}.$$

C2 The following matrices

$$\begin{bmatrix} \alpha_{i_1}^{c_1} & \alpha_{i_1}^{c_2} & \dots & \alpha_{i_1}^{c_T} \\ \alpha_{i_2}^{c_1} & \alpha_{i_2}^{c_2} & \dots & \alpha_{i_2}^{c_T} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{i_T}^{c_1} & \alpha_{i_T}^{c_2} & \dots & \alpha_{i_T}^{c_T} \end{bmatrix}_{T \times T}, \quad \begin{bmatrix} \alpha_{i_1}^{d_1} & \alpha_{i_1}^{d_2} & \dots & \alpha_{i_1}^{d_T} \\ \alpha_{i_2}^{d_1} & \alpha_{i_2}^{d_2} & \dots & \alpha_{i_2}^{d_T} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{i_T}^{d_1} & \alpha_{i_T}^{d_2} & \dots & \alpha_{i_T}^{d_T} \end{bmatrix}_{T \times T} \quad (9)$$

are non-singular over \mathbb{F}_q for any $\mathcal{T} = \{i_1, \dots, i_T\} \subseteq [N]$ with $|\mathcal{T}| = T$, where $\alpha_1, \alpha_2, \dots, \alpha_N$ are N pairwise distinct non-zero elements from \mathbb{F}_q .

To complete the computation $\mathbf{C} = \mathbf{AB}$ (6), the master first shares the evaluations of $f_P(x)$ and $h_P(x)$ at $x = \alpha_i$ with worker $i \in [N]$. Then the worker i computes the product $f_P(\alpha_i) \cdot h_P(\alpha_i)$ and sends it back to the master on successful completion, which is equivalent to evaluating of the polynomial $g(x) = f_P(x) \cdot h_P(x)$ at $x = \alpha_i$. Thus, the master can interpolate $g(x)$ from any $K = \delta + 1$ responses by using Lagrange interpolation rule, and then recovers all the desired products of sub-matrices $\mathbf{C}_{k,j}, k \in [m], j \in [n]$ from the coefficients of $g(x)$ by C1. The matrices \mathbf{A} and \mathbf{B} are secure against any T colluding workers by C2 and Lemma 1. Therefore, the SMM strategy based on polynomial codes achieves the recovery threshold $K = \delta + 1$.

As far as we know, the state-of-the-art strategies for SMM based on polynomial codes are reflected in [11], [15], which are summarized in the following lemma.

Lemma 2. *For any arbitrary partitioning of matrices \mathbf{A} and \mathbf{B} with parameters m, p, n , the state-of-the-art strategies for SMM based on polynomial codes achieve*

- the recovery threshold $K = (m+1)(np+T) - 1$ [15] by setting $a_{k,\ell} = (k-1)(np+T) + \ell - 1$, $b_{\ell,j} = jp - \ell$, $c_t = (m-1)(np+T) + np + t - 1$, $d_t = np + t - 1$ for all $k \in [m]$, $\ell \in [p]$, $j \in [n]$, $t \in [T]$,
- the recovery threshold $K = (n+1)(mp+T) - 1$ [15] by setting $a_{k,\ell} = (k-1)p + \ell - 1$, $b_{\ell,j} = (j-1)(mp+T) + p - \ell$, $c_t = mp + t - 1$, $d_t = (n-1)(mp+T) + mp + t - 1$ for all $k \in [m]$, $\ell \in [p]$, $j \in [n]$, $t \in [T]$,
- and the recovery threshold $K = 2mpn + 2T - 1$ [11] by setting $a_{k,\ell} = (k-1)np + \ell - 1$, $b_{\ell,j} = jp - \ell$, $c_t = mpn + t - 1$, $d_t = mpn + t - 1$ for all $k \in [m]$, $\ell \in [p]$, $j \in [n]$, $t \in [T]$.

That is, the current best SMM strategies based on polynomial codes achieve the recovery threshold $K = \min\{(m+1)(np+T) - 1, (n+1)(mp+T) - 1, 2mpn + 2T - 1\}$.

B. Secure Matrix Multiplication Based on Lagrange Codes

Lagrange codes were originally introduced in [22] and is widely applied to solve batch processing problems for coded distributed computing [17], [19]. To solve SMM using Lagrange codes [16], [20], matrix multiplication is first converted into the problem of computing the element-wise product of two batches of sub-matrices, by employing the concept of bilinear complexity, and then Lagrange codes can directly operate on the problem of batch sub-matrix multiplication.

Definition 1 (Bilinear Complexity [45], [46]). Let $\mathbf{C} = [C_{k,j}]_{k \in [m], j \in [n]}$ be the product of any matrices $\mathbf{A} = [A_{k,\ell}]_{k \in [m], \ell \in [p]}$ and $\mathbf{B} = [B_{\ell,j}]_{\ell \in [p], j \in [n]}$, where $C_{k,j} = \sum_{\ell=1}^p A_{k,\ell} B_{\ell,j}$. The bilinear complexity, denoted by $R(m, p, n)$, is defined as the minimum number of active multiplications for the problem of multiplying the two matrices \mathbf{A} and \mathbf{B} . Moreover, an upper bound construction with rank R for bilinear complexity² means that, there exists tensors $a \in \mathbb{F}_q^{R \times m \times p}$, $b \in \mathbb{F}_q^{R \times p \times n}$, $c \in \mathbb{F}_q^{R \times m \times n}$ satisfying

$$\begin{aligned} \sum_{r=1}^R c_{r,k,j} \left(\underbrace{\sum_{k'=1}^m \sum_{\ell'=1}^p a_{r,k',\ell'} A_{k',\ell'}}_{=A_r} \right) \left(\underbrace{\sum_{\ell'=1}^p \sum_{j'=1}^n b_{r,\ell',j'} B_{\ell',j'}}_{=B_r} \right) \\ = \sum_{\ell=1}^p A_{k,\ell} B_{\ell,j} = C_{k,j}, \quad \forall k \in [m], j \in [n]. \end{aligned}$$

It is straightforward to observe from Definition 1 that, bilinear complexity enables converting the matrix multiplication problem $\mathbf{C} = \mathbf{AB}$ in (6) into computing the element-wise products of two batches of sub-matrices of length R . Specifically, given any upper bound construction for bilinear complexity with tensors $a = (a_{r,k,\ell})$, $b = (b_{r,\ell,j})$, $c = (c_{r,k,j})$ and rank R , the desired products of sub-matrices $\mathbf{C}_{k,j}$ can be recovered by

$$\sum_{r=1}^R c_{r,k,j} \mathbf{A}_r \mathbf{B}_r = \sum_{\ell=1}^p \mathbf{A}_{k,\ell} \mathbf{B}_{\ell,j} = \mathbf{C}_{k,j}, \quad \forall k \in [m], j \in [n], \quad (10)$$

²The upper bound construction of bilinear complexity is known for many cases of parameters m, p, n , based on the recursive method in [45].

if one obtains the element-wise product $\{\mathbf{A}_r \mathbf{B}_r : r \in [R]\}$ of the two batches of sub-matrices $(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_R)$ and $(\mathbf{B}_1, \mathbf{B}_2, \dots, \mathbf{B}_R)$, where

$$\mathbf{A}_r = \sum_{k=1}^m \sum_{\ell=1}^p a_{r,k,\ell} \mathbf{A}_{k,\ell}, \quad \forall r \in [R], \quad (11)$$

$$\mathbf{B}_r = \sum_{\ell=1}^p \sum_{j=1}^n b_{r,\ell,j} \mathbf{B}_{\ell,j}, \quad \forall r \in [R]. \quad (12)$$

That is, bilinear complexity converts the matrix multiplication $\mathbf{C} = \mathbf{AB}$ into the problem of computing the element-wise product of two batches of sub-matrices $(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_R)$ and $(\mathbf{B}_1, \mathbf{B}_2, \dots, \mathbf{B}_R)$. Then Lagrange codes are operated as follows.

Let $\{\beta_r, \alpha_i : r \in [R+T], i \in [N]\}$ be $R+T+N$ distinct elements from \mathbb{F}_q . Construct the encoding functions $f_L(x)$ and $h_L(x)$ of the two batches of sub-matrices as Lagrange interpolation polynomials of degree $R+T-1$, such that

$$f_L(\beta_r) = \begin{cases} \mathbf{A}_r, & \forall r \in [R] \\ \mathbf{Z}_r^{\mathbf{A}}, & \forall r \in [R+1 : R+T] \end{cases} \quad (13)$$

$$h_L(\beta_r) = \begin{cases} \mathbf{B}_r, & \forall r \in [R] \\ \mathbf{Z}_r^{\mathbf{B}}, & \forall r \in [R+1 : R+T] \end{cases}, \quad (14)$$

where $\mathbf{Z}_{R+1}^{\mathbf{A}}, \dots, \mathbf{Z}_{R+T}^{\mathbf{A}}$ and $\mathbf{Z}_{R+1}^{\mathbf{B}}, \dots, \mathbf{Z}_{R+T}^{\mathbf{B}}$ are random matrices over \mathbb{F}_q with the same dimensions as \mathbf{A}_r and \mathbf{B}_r , respectively. By Lagrange interpolation rule, the polynomials $f_L(x)$ and $h_L(x)$ are written as

$$\begin{aligned} f_L(x) = \sum_{r=1}^R \mathbf{A}_r \cdot \prod_{j \in [R+T] \setminus \{r\}} \frac{x - \beta_j}{\beta_r - \beta_j} \\ + \sum_{k=R+1}^{R+T} \mathbf{Z}_k^{\mathbf{A}} \cdot \prod_{j \in [R+T] \setminus \{k\}} \frac{x - \beta_j}{\beta_k - \beta_j}, \end{aligned} \quad (15)$$

$$\begin{aligned} h_L(x) = \sum_{r=1}^R \mathbf{B}_r \cdot \prod_{j \in [R+T] \setminus \{r\}} \frac{x - \beta_j}{\beta_r - \beta_j} \\ + \sum_{k=R+1}^{R+T} \mathbf{Z}_k^{\mathbf{B}} \cdot \prod_{j \in [R+T] \setminus \{k\}} \frac{x - \beta_j}{\beta_k - \beta_j}. \end{aligned} \quad (16)$$

To complete computation, the master first shares the evaluations of $f_L(x)$ and $h_L(x)$ at point $x = \alpha_i$ with worker $i \in [N]$, who then responds with the product $f_L(\alpha_i) \cdot h_L(\alpha_i)$. Apparently, the master can interpolate the product polynomial $g(x) = f_L(x) \cdot h_L(x)$ from any $K = \deg(g(x)) + 1 = 2R + 2T - 1$ responses, and then evaluates $g(x)$ at $x = \beta_1, \beta_2, \dots, \beta_R$ to obtain the element-wise product $\{\mathbf{A}_r \mathbf{B}_r : r \in [R]\}$ by (13)-(14). It is straightforward to prove the security of \mathbf{A} and \mathbf{B} by Lemma 1. Hence, the SMM strategy based on Lagrange codes achieves the recovery threshold $K = 2R + 2T - 1$.

IV. MAIN RESULTS

We state our main results in this section. For brevity, we focus on the results of recovery threshold, and present the communication costs and computation complexities of

proposed strategies for PSMM (resp. FPMM) in Section V-C (resp. VI-C).

Theorem 1. *For the problem of private and secure matrix multiplication with T colluding workers and the partitioning parameters m, p, n , give any positive integers $\{a_{k,\ell}, b_{\ell,j}, c_t, d_t : k \in [m], \ell \in [p], j \in [n], t \in [T]\}$ satisfying C1-C2, there exists a computation strategy based on polynomial codes that achieves a recovery threshold of $K = \max\{a_{k,\ell}, c_t : k \in [m], \ell \in [p], t \in [T]\} + \max\{b_{\ell,j}, d_t : \ell \in [p], j \in [n], t \in [T]\} + 1$.*

Theorem 1 is proved in Section V-A by presenting our proposed PSMM strategy based on polynomial codes. The confidential matrix \mathbf{A} and index θ are secured by polynomial codes such that the response computed at each worker resembles that of the SMM strategy in Section III-A.

From Lemma 2, we can directly obtain the following corollary of Theorem 1.

Corollary 1. *The recovery threshold $K = \min\{(m+1)(np+T)-1, (n+1)(mp+T)-1, 2mpn+2T-1\}$ can be achieved by some PSMM strategy based on polynomial codes.*

Remark 1. While the recovery threshold presented in Corollary 1 is obtained by adopting the degree parameters in Lemma 2 for the underlying polynomial codes, we can flexibly optimize system performance over degree parameters $\{a_{k,\ell}, b_{\ell,j}, c_t, d_t : k \in [m], \ell \in [p], j \in [n], t \in [T]\}$ that satisfy conditions C1-C2. This remains to be an interesting future research problem.

Theorem 2. *For the problem of private and secure matrix multiplication with T colluding workers and the partitioning parameters m, p, n , there exists a computation strategy based on Lagrange codes that achieves a recovery threshold of $K = 2R + 2T - 1$, where R denotes the rank of any construction for bilinear complexity of multiplying an m -by- p matrix and a p -by- n matrix.*

Theorem 2 is proved in Section V-B by constructing a PSMM strategy based on Lagrange codes. The confidential matrix \mathbf{A} and index θ are secured by Lagrange codes such that the response computed at each worker resembles that of the SMM strategy in Section III-B.

Remark 2. As far as we know, the general upper bound construction R for bilinear complexity remains open. Reference [50] lists the current best known upper construction of bilinear complexity for almost all possible partitioning parameters m, p, n with $m \in [2 : 32], m \leq p \leq n \leq 32$. For some specific combinations of parameters (m, p, n) , we compare the recovery thresholds achieved by our proposed PSMM strategies in Table I. For each specific combination of (m, p, n) , which strategy achieves a smaller recovery threshold depends on the value of the security parameter T . For example, for the parameter case of $(m = 3, p = 3, n = 3)$, the PSMM strategy based on polynomial codes outperforms the one based on Lagrange codes in terms of recovery threshold when $T < 5$. A similar discussion holds for the following FPMM strategies based on polynomial codes and Lagrange codes. The detailed comparisons between the two proposed strategies for PSMM

and FPMM problems are presented in Sections V-C4 and VI-C4, respectively.

We next turn to present the results of recovery thresholds achieved by our proposed strategies, for the fully private matrix multiplication problem.

Theorem 3. *For the problem of fully private matrix multiplication with T colluding workers and the partitioning parameters m, p, n , give any positive integers $\{a_{k,\ell}, b_{\ell,j}, c_t, d_t : k \in [m], \ell \in [p], j \in [n], t \in [T]\}$ satisfying C1-C2, there exists a computation strategy based on polynomial codes that achieves a recovery threshold of $K = \max\{a_{k,\ell}, c_t : k \in [m], \ell \in [p], t \in [T]\} + \max\{b_{\ell,j}, d_t : \ell \in [p], j \in [n], t \in [T]\} + 1$.*

Theorem 3 is proved in Section VI-A by presenting a FPMM strategy based on polynomial codes. The confidential matrix indices θ_1 and θ_2 are secured by polynomial codes such that the response computed at each worker resembles that of the SMM strategy in Section III-A.

The following corollary is immediate from Lemma 2.

Corollary 2. *The recovery threshold $K = \min\{(m+1)(np+T)-1, (n+1)(mp+T)-1, 2mpn+2T-1\}$ can be achieved by some FPMM strategy based on polynomial codes.*

Theorem 4. *For the problem of fully private matrix multiplication with T colluding workers and the partitioning parameters m, p, n , there exists a computation strategy based on Lagrange codes that achieves a recovery threshold of $K = 2R + 2T - 1$, where R denotes the rank of any construction for bilinear complexity of multiplying an m -by- p matrix and a p -by- n matrix.*

Theorem 4 is proved in Section VI-B by presenting a FPMM strategy based on Lagrange codes. The confidential matrix indices θ_1 and θ_2 are secured by Lagrange codes such that the response computed at each worker resembles that of the SMM strategy in Section III-B.

Remark 3. We may further consider the presence of some adversarial workers of size E who maliciously return arbitrarily erroneous responses to the master. In our proposed strategies for PSMM and FPMM, the responses of all the workers can be viewed as evaluations of a polynomial at distinct points, and accordingly the responses constitute a Reed-Solomon codeword. Thus, our proposed strategies can provide robustness against the E adversarial workers by waiting for responses from $2E$ more workers.

V. COMPUTATION STRATEGIES FOR PRIVATE AND SECURE MATRIX MULTIPLICATION

In this section, we first present two PSMM strategies, which are constructed by exploiting the structure of SMM strategies based on polynomial codes and Lagrange codes, respectively. Then their security, privacy, communication cost and computation complexities are analysed. This provides proofs for Theorems 1 and 2.

To better attain the tradeoff with respect to system performance, similar to (5), the matrices \mathbf{A} and $\mathbf{B}^{(v)}$ are divided

TABLE I
RECOVERY THRESHOLDS OF THE PROPOSED PSMM STRATEGIES BASED ON POLYNOMIAL CODES AND LAGRANGE CODES.

Partitioning Parameters	Best Known Bilinear Complexity R [50]	Recovery Threshold for PSMM	
		Polynomial codes Based	Lagrange codes Based
$m = 2, p = 2, n = 2$	7	$\min\{11 + 3T, 15 + 2T\}$	$13 + 2T$
$m = 3, p = 3, n = 3$	23	$\min\{35 + 4T, 53 + 2T\}$	$45 + 2T$
$m = 5, p = 5, n = 5$	98	$\min\{149 + 6T, 249 + 2T\}$	$195 + 2T$

into $m \times p$ and $p \times n$ equal-size sub-matrices, respectively, for any partitioning parameters m, p, n , i.e., for all $v \in [V]$,

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_{1,1} & \cdots & \mathbf{A}_{1,p} \\ \vdots & \ddots & \vdots \\ \mathbf{A}_{m,1} & \cdots & \mathbf{A}_{m,p} \end{bmatrix}, \quad \mathbf{B}^{(v)} = \begin{bmatrix} \mathbf{B}_{1,1}^{(v)} & \cdots & \mathbf{B}_{1,n}^{(v)} \\ \vdots & \ddots & \vdots \\ \mathbf{B}_{p,1}^{(v)} & \cdots & \mathbf{B}_{p,n}^{(v)} \end{bmatrix}, \quad (17)$$

where $\mathbf{A}_{k,\ell} \in \mathbb{F}_q^{\frac{\lambda}{p} \times \frac{\omega}{p}}$ for any $k \in [m], \ell \in [p]$, and $\mathbf{B}_{\ell,j}^{(v)} \in \mathbb{F}_q^{\frac{\omega}{p} \times \frac{\gamma}{n}}$ for any $\ell \in [p], j \in [n]$. Then the desired product $\mathbf{C}^{(\theta)} = \mathbf{A}\mathbf{B}^{(\theta)}$ is given by

$$\mathbf{C}^{(\theta)} = \mathbf{A}\mathbf{B}^{(\theta)} = \begin{bmatrix} \mathbf{C}_{1,1}^{(\theta)} & \cdots & \mathbf{C}_{1,n}^{(\theta)} \\ \vdots & \ddots & \vdots \\ \mathbf{C}_{m,1}^{(\theta)} & \cdots & \mathbf{C}_{m,n}^{(\theta)} \end{bmatrix}$$

with $\mathbf{C}_{k,j}^{(\theta)} = \sum_{\ell=1}^p \mathbf{A}_{k,\ell} \mathbf{B}_{\ell,j}^{(\theta)}$ for any $k \in [m], j \in [n]$.

A. PSMM Strategy Based on Polynomial Codes

We start with proving Theorem 1. We show that any SMM strategy based on polynomial codes can be exploited to construct a PSMM strategy with same recovery threshold. First, we illustrate the key idea behind the proposed PSMM strategy through a simple example.

Example 1. We consider a PSMM problem with $V = m = p = n = T = 2$. The matrices \mathbf{A} and $\mathbf{B}^{(1)}, \mathbf{B}^{(2)}$ are partitioned as

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_{1,1} & \mathbf{A}_{1,2} \\ \mathbf{A}_{2,1} & \mathbf{A}_{2,2} \end{bmatrix}, \mathbf{B}^{(1)} = \begin{bmatrix} \mathbf{B}_{1,1}^{(1)} & \mathbf{B}_{1,2}^{(1)} \\ \mathbf{B}_{2,1}^{(1)} & \mathbf{B}_{2,2}^{(1)} \end{bmatrix}, \mathbf{B}^{(2)} = \begin{bmatrix} \mathbf{B}_{1,1}^{(2)} & \mathbf{B}_{1,2}^{(2)} \\ \mathbf{B}_{2,1}^{(2)} & \mathbf{B}_{2,2}^{(2)} \end{bmatrix}. \quad (18)$$

Assume that the master wishes to privately compute $\mathbf{C}^{(1)} = \mathbf{A}\mathbf{B}^{(1)}$, which is given by

$$\begin{aligned} \mathbf{C}^{(1)} &= \begin{bmatrix} \mathbf{C}_{1,1}^{(1)} & \mathbf{C}_{1,2}^{(1)} \\ \mathbf{C}_{2,1}^{(1)} & \mathbf{C}_{2,2}^{(1)} \end{bmatrix} \\ &= \begin{bmatrix} \mathbf{A}_{1,1}\mathbf{B}_{1,1}^{(1)} + \mathbf{A}_{1,2}\mathbf{B}_{2,1}^{(1)} & \mathbf{A}_{1,1}\mathbf{B}_{1,2}^{(1)} + \mathbf{A}_{1,2}\mathbf{B}_{2,2}^{(1)} \\ \mathbf{A}_{2,1}\mathbf{B}_{1,1}^{(1)} + \mathbf{A}_{2,2}\mathbf{B}_{2,1}^{(1)} & \mathbf{A}_{2,1}\mathbf{B}_{1,2}^{(1)} + \mathbf{A}_{2,2}\mathbf{B}_{2,2}^{(1)} \end{bmatrix}. \end{aligned} \quad (19)$$

Consider an SMM strategy based on polynomial codes with recovery threshold $K = 17$ and the following assignment [15]:

$$\begin{aligned} a_{1,1} &= 0, \quad a_{1,2} = 1, \quad a_{2,1} = 6, \quad a_{2,2} = 7, \quad c_1 = 10, \quad c_2 = 11, \\ b_{1,1} &= 1, \quad b_{1,2} = 3, \quad b_{2,1} = 0, \quad b_{2,2} = 2, \quad d_1 = 4, \quad d_2 = 5. \end{aligned}$$

Then the encoding functions of \mathbf{A} and $\mathbf{B}^{(1)}$ are in the forms of

$$f_{\mathbf{A}}(x) = \mathbf{A}_{1,1} + \mathbf{A}_{1,2}x + \mathbf{A}_{2,1}x^6 + \mathbf{A}_{2,2}x^7 + \mathbf{Z}_1^{\mathbf{A}}x^{10} + \mathbf{Z}_2^{\mathbf{A}}x^{11}, \quad (20)$$

$$h_{\mathbf{B}}(x) = \mathbf{B}_{2,1}^{(1)} + \mathbf{B}_{1,1}^{(1)}x + \mathbf{B}_{2,2}^{(1)}x^2 + \mathbf{B}_{1,2}^{(1)}x^3 + \mathbf{Z}_1^{\mathbf{B}}x^4 + \mathbf{Z}_2^{\mathbf{B}}x^5, \quad (21)$$

where $\mathbf{Z}_1^{\mathbf{A}}, \mathbf{Z}_2^{\mathbf{A}}$ and $\mathbf{Z}_1^{\mathbf{B}}, \mathbf{Z}_2^{\mathbf{B}}$ are the matrices with corresponding dimensions and will be specified later. The computation $\mathbf{C}^{(1)}$ can be completed by interpolating the polynomial $g(x) = \sum_{r=0}^{16} g_r x^r = f_{\mathbf{A}}(x) \cdot h_{\mathbf{B}}(x)$ because

$$g_1 = \mathbf{A}_{1,1}\mathbf{B}_{1,1}^{(1)} + \mathbf{A}_{1,2}\mathbf{B}_{2,1}^{(1)} = \mathbf{C}_{1,1}^{(1)},$$

$$g_3 = \mathbf{A}_{1,1}\mathbf{B}_{1,2}^{(1)} + \mathbf{A}_{1,2}\mathbf{B}_{2,2}^{(1)} = \mathbf{C}_{1,2}^{(1)},$$

$$g_7 = \mathbf{A}_{2,1}\mathbf{B}_{1,1}^{(1)} + \mathbf{A}_{2,2}\mathbf{B}_{2,1}^{(1)} = \mathbf{C}_{2,1}^{(1)},$$

$$g_9 = \mathbf{A}_{2,1}\mathbf{B}_{1,2}^{(1)} + \mathbf{A}_{2,2}\mathbf{B}_{2,2}^{(1)} = \mathbf{C}_{2,2}^{(1)}.$$

In PSMM, to ensure security, let $\mathbf{Z}_1^{\mathbf{A}}, \mathbf{Z}_2^{\mathbf{A}}$ be independently and uniformly random matrices over \mathbb{F}_q . Then the master shares $\tilde{\mathbf{A}}_i = f_{\mathbf{A}}(\alpha_i)$ with worker i , where $\alpha_1, \alpha_2, \dots, \alpha_N$ are pairwise distinct non-zero elements from \mathbb{F}_q . Along with $\tilde{\mathbf{A}}_i$, for the partitioning sub-matrices $\mathbf{B}_{\ell,j}^{(1)}$ and $\mathbf{B}_{\ell,j}^{(2)}$, the master also shares with the queries $q_{\ell,j}^{(1)}(\alpha_i)$ and $q_{\ell,j}^{(2)}(\alpha_i)$, respectively, for all $\ell, j = 1, 2$, which are given by

$$\begin{aligned} q_{\ell,j}^{(1)}(\alpha_i) &= \alpha_i^{b_{\ell,j}} + z_{\ell,j,1}^{(1)} \cdot \alpha_i^4 + z_{\ell,j,2}^{(1)} \cdot \alpha_i^5, \\ q_{\ell,j}^{(2)}(\alpha_i) &= z_{\ell,j,1}^{(2)} \cdot \alpha_i^4 + z_{\ell,j,2}^{(2)} \cdot \alpha_i^5, \end{aligned}$$

where $z_{\ell,j,1}^{(1)}, z_{\ell,j,2}^{(1)}$ and $z_{\ell,j,1}^{(2)}, z_{\ell,j,2}^{(2)}$ are uniformly random noises in \mathbb{F}_q that protect $T = 2$ colluding privacy. Upon the queries, each worker i encodes $\mathbf{B}^{(1)}, \mathbf{B}^{(2)}$ into

$$\begin{aligned} \tilde{\mathbf{B}}_i &= \mathbf{B}_{1,1}^{(1)}q_{1,1}^{(1)}(\alpha_i) + \mathbf{B}_{1,2}^{(1)}q_{1,2}^{(1)}(\alpha_i) + \mathbf{B}_{2,1}^{(1)}q_{2,1}^{(1)}(\alpha_i) \\ &\quad + \mathbf{B}_{2,2}^{(1)}q_{2,2}^{(1)}(\alpha_i) + \mathbf{B}_{1,1}^{(2)}q_{1,1}^{(2)}(\alpha_i) + \mathbf{B}_{1,2}^{(2)}q_{1,2}^{(2)}(\alpha_i) \\ &\quad + \mathbf{B}_{2,1}^{(2)}q_{2,1}^{(2)}(\alpha_i) + \mathbf{B}_{2,2}^{(2)}q_{2,2}^{(2)}(\alpha_i) \\ &= \mathbf{B}_{2,1}^{(1)} + \mathbf{B}_{1,1}^{(1)}\alpha_i + \mathbf{B}_{2,2}^{(1)}\alpha_i^2 + \mathbf{B}_{1,2}^{(1)}\alpha_i^3 + \mathbf{Z}_1^{\mathbf{B}}\alpha_i^4 + \mathbf{Z}_2^{\mathbf{B}}\alpha_i^5 \\ &= h_{\mathbf{B}}(\alpha_i), \end{aligned}$$

where we set $\mathbf{Z}_t^{\mathbf{B}} = \mathbf{B}_{1,1}^{(1)}z_{1,1,t}^{(1)} + \mathbf{B}_{1,2}^{(1)}z_{1,2,t}^{(1)} + \mathbf{B}_{2,1}^{(1)}z_{2,1,t}^{(1)} + \mathbf{B}_{2,2}^{(1)}z_{2,2,t}^{(1)} + \mathbf{B}_{1,1}^{(2)}z_{1,1,t}^{(2)} + \mathbf{B}_{1,2}^{(2)}z_{1,2,t}^{(2)} + \mathbf{B}_{2,1}^{(2)}z_{2,1,t}^{(2)} + \mathbf{B}_{2,2}^{(2)}z_{2,2,t}^{(2)}$ for any $t = 1, 2$ that is constant for all workers and align interference to the dimension corresponding to x^4 if $t = 1$ or x^5 if $t = 2$, similar to (21).

Each worker i computes $\tilde{\mathbf{A}}_i \tilde{\mathbf{B}}_i$ as a response, which can be viewed as evaluating of $g(x) = f_{\mathbf{A}}(x) \cdot h_{\mathbf{B}}(x)$ at point $x = \alpha_i$. Hence, the master can interpolate the product $g(x)$ from any $K = \deg(g(x)) + 1 = 17$ responses, and recover the desired computation $\mathbf{A}\mathbf{B}^{(1)}$.

Next, we formally describe the general PSMM construction based on polynomial codes. Let the positive integers $\{a_{k,\ell}, b_{\ell,j}, c_t, d_t : k \in [m], \ell \in [p], j \in [n], t \in [T]\}$ satisfying C1-C2 be the parameters of the SMM strategy based on polynomial codes. To ensure the security of its own matrix

\mathbf{A} (17), the master employs the encoding function defined in (7) to encode \mathbf{A} as

$$f_{\mathbf{A}}(x) = \sum_{k=1}^m \sum_{\ell=1}^p \mathbf{A}_{k,\ell} x^{a_{k,\ell}} + \sum_{t=1}^T \mathbf{Z}_t^{\mathbf{A}} x^{c_t}, \quad (22)$$

where $\mathbf{Z}_1^{\mathbf{A}}, \dots, \mathbf{Z}_T^{\mathbf{A}}$ are the random matrices over \mathbb{F}_q with the same dimension as $\mathbf{A}_{k,\ell}$.

To keep the index θ private, the master generates $VTpn$ random noises $\{z_{\ell,j,t}^{(v)} : \ell \in [p], j \in [n], v \in [V], t \in [T]\}$ independently and uniformly from \mathbb{F}_q . Then based on the structure of the encoding function defined in (8), construct the query polynomial $q_{\ell,j}^{(v)}(x)$ for any $\ell \in [p], j \in [n], v \in [V]$ as

$$q_{\ell,j}^{(v)}(x) = \sum_{t=1}^T z_{\ell,j,t}^{(v)} \cdot x^{d_t} + \begin{cases} x^{b_{\ell,j}}, & \text{if } v = \theta \\ 0, & \text{if } v \neq \theta \end{cases}. \quad (23)$$

Here the number of the query polynomials is deliberately designed to be equal to the number of the partitioning sub-matrices in the library $\mathcal{L}^{\mathbf{B}}$. In particular, each query polynomial $q_{\ell,j}^{(v)}(x)$ corresponds to the sub-matrix $\mathbf{B}_{\ell,j}^{(v)}$ for any $\ell \in [p], j \in [n], v \in [V]$, and will be used as encoding coefficient to encode $\mathbf{B}_{\ell,j}^{(v)}$, as shown in (26). When $v = \theta$, the sub-matrix $\mathbf{B}_{\ell,j}^{(v)}$ is desired to be computed and the coefficient $x^{b_{\ell,j}}$ is used to encode $\mathbf{B}_{\ell,j}^{(v)}$ in the same sense as the encoding function in (8). When $v \neq \theta$, the coefficient 0 is used to eliminate interference from the undesired sub-matrix $\mathbf{B}_{\ell,j}^{(v)}$. Moreover, the term $\sum_{t=1}^T z_{\ell,j,t}^{(v)} \cdot x^{d_t}$ is to provide robustness against T colluding privacy, and to align interference from all the partitioning sub-matrices in $\mathcal{L}^{\mathbf{B}}$ (see (29)) since it has identical structure across all these partitioning sub-matrices.

Let $\alpha_1, \alpha_2, \dots, \alpha_N$ be the pairwise distinct non-zero elements in \mathbb{F}_q . The master shares the evaluations of $f_{\mathbf{A}}(x)$ and $\{q_{\ell,j}^{(v)}(x) : \ell \in [p], j \in [n], v \in [V]\}$ at point $x = \alpha_i$ with worker i , i.e.,

$$\tilde{\mathbf{A}}_i = f_{\mathbf{A}}(\alpha_i), \quad (24)$$

$$\mathcal{Q}_i^{(\theta)} = \{q_{\ell,j}^{(v)}(\alpha_i) : \ell \in [p], j \in [n], v \in [V]\}. \quad (25)$$

After receiving the query $\mathcal{Q}_i^{(\theta)}$, worker i encodes the matrices $\mathbf{B}^{([V])}$ by taking a linear combination of the elements in $\mathcal{Q}_i^{(\theta)}$ and all the partitioning sub-matrices of $\mathbf{B}^{([V])}$ (17), given by

$$\tilde{\mathbf{B}}_i = \sum_{v=1}^V \sum_{\ell=1}^p \sum_{j=1}^n \mathbf{B}_{\ell,j}^{(v)} \cdot q_{\ell,j}^{(v)}(\alpha_i). \quad (26)$$

Denote the encoding function of $\mathbf{B}^{([V])}$ by

$$\begin{aligned} h_{\mathbf{B}}(x) &= \sum_{v=1}^V \sum_{\ell=1}^p \sum_{j=1}^n \mathbf{B}_{\ell,j}^{(v)} \cdot q_{\ell,j}^{(v)}(x) \\ &\stackrel{(a)}{=} \sum_{\ell=1}^p \sum_{j=1}^n \mathbf{B}_{\ell,j}^{(\theta)} x^{b_{\ell,j}} + \sum_{v=1}^V \sum_{\ell=1}^p \sum_{j=1}^n \mathbf{B}_{\ell,j}^{(v)} \cdot \sum_{t=1}^T z_{\ell,j,t}^{(v)} x^{d_t} \\ &= \sum_{\ell=1}^p \sum_{j=1}^n \mathbf{B}_{\ell,j}^{(\theta)} x^{b_{\ell,j}} + \sum_{t=1}^T x^{d_t} \cdot \sum_{v=1}^V \sum_{\ell=1}^p \sum_{j=1}^n \mathbf{B}_{\ell,j}^{(v)} z_{\ell,j,t}^{(v)} \end{aligned} \quad (27)$$

$$= \sum_{\ell=1}^p \sum_{j=1}^n \mathbf{B}_{\ell,j}^{(\theta)} x^{b_{\ell,j}} + \sum_{t=1}^T \mathbf{Z}_t^{\mathbf{B}} x^{d_t}, \quad (28)$$

where (a) follows by (23), and

$$\mathbf{Z}_t^{\mathbf{B}} = \sum_{v=1}^V \sum_{\ell=1}^p \sum_{j=1}^n \mathbf{B}_{\ell,j}^{(v)} z_{\ell,j,t}^{(v)}, \quad \forall t \in [T] \quad (29)$$

which are identical for all workers and thus can be viewed as constant terms.

We can observe from (28)-(29) that, the encoding function $h_{\mathbf{B}}(x)$ of $\mathbf{B}^{([V])}$ efficiently separates the desired sub-matrices and the interference in the same structure as the encoding function in (8), where the desired sub-matrices $\{\mathbf{B}_{\ell,j}^{(\theta)}\}_{\ell \in [p], j \in [n]}$ appear along the pn dimensions corresponding to $\{x^{b_{\ell,j}}\}_{\ell \in [p], j \in [n]}$ and the interference from all the partitioning sub-matrices of $\mathbf{B}^{([V])}$ is aligned along the T dimensions corresponding to $\{x^{d_t}\}_{t \in [T]}$. Thus, we have the fact from the SMM strategy based on polynomial codes in Section III-A that, the desired computation $\mathbf{C}^{(\theta)} = \mathbf{A}\mathbf{B}^{(\theta)}$ can be recovered from the product polynomial $g(x) = f_{\mathbf{A}}(x) \cdot h_{\mathbf{B}}(x)$.

Next, each worker i computes the product

$$\mathbf{Y}_i^{(\theta)} = \tilde{\mathbf{A}}_i \tilde{\mathbf{B}}_i \quad (30)$$

and send it back to the master, which is equivalent to evaluating of the polynomial $g(x) = f_{\mathbf{A}}(x) \cdot h_{\mathbf{B}}(x)$ at point $x = \alpha_i$ by (24) and (26)-(27). Thus, the master can interpolate $g(x)$ from the responses of any $K = \deg(g(x)) + 1 = \max\{a_{k,\ell}, c_t : k \in [m], \ell \in [p], t \in [T]\} + \max\{b_{\ell,j}, d_t : \ell \in [p], j \in [n], t \in [T]\} + 1$ workers and then recovers $\mathbf{C}^{(\theta)} = \mathbf{A}\mathbf{B}^{(\theta)}$.

B. PSMM Strategy Based on Lagrange Codes

Now we state the strategy that proves Theorem 2. We will show that, given any upper bound construction $a = (a_{r,k,\ell}), b = (b_{r,\ell,j}), c = (c_{r,k,j})$ with rank R for bilinear complexity of multiplying an m -by- p matrix and a p -by- n matrix, the SMM strategy based on Lagrange codes can be exploited to construct a PSMM strategy with same recovery threshold. Let us start with an example to illustrate the idea.

Example 2. Consider the same parameters as Example 1, i.e., $V = m = p = n = T = 2$. The partitions of matrices $\mathbf{A}, \mathbf{B}^{(1)}, \mathbf{B}^{(2)}$ and the desired computation $\mathbf{C}^{(1)} = \mathbf{A}\mathbf{B}^{(1)}$ are shown in (18) and (19), respectively.

Firstly, we use Strassen's construction [46] with bilinear complexity $R = 7$ to encode the sub-matrices of \mathbf{A} and $\mathbf{B}^{(1)}, \mathbf{B}^{(2)}$ as

$$\begin{aligned} \mathbf{A}_1 &= \mathbf{A}_{1,1} + \mathbf{A}_{2,2}, & \mathbf{B}_1^{(1)} &= \mathbf{B}_{1,1}^{(1)} + \mathbf{B}_{2,2}^{(1)}, & \mathbf{B}_1^{(2)} &= \mathbf{B}_{1,1}^{(2)} + \mathbf{B}_{2,2}^{(2)}, \\ \mathbf{A}_2 &= \mathbf{A}_{2,1} + \mathbf{A}_{2,2}, & \mathbf{B}_2^{(1)} &= \mathbf{B}_{1,1}^{(1)}, & \mathbf{B}_2^{(2)} &= \mathbf{B}_{1,1}^{(2)}, \\ \mathbf{A}_3 &= \mathbf{A}_{1,1}, & \mathbf{B}_3^{(1)} &= \mathbf{B}_{1,2}^{(1)} - \mathbf{B}_{2,2}^{(1)}, & \mathbf{B}_3^{(2)} &= \mathbf{B}_{1,2}^{(2)} - \mathbf{B}_{2,2}^{(2)}, \\ \mathbf{A}_4 &= \mathbf{A}_{2,2}, & \mathbf{B}_4^{(1)} &= \mathbf{B}_{2,1}^{(1)} - \mathbf{B}_{1,1}^{(1)}, & \mathbf{B}_4^{(2)} &= \mathbf{B}_{2,1}^{(2)} - \mathbf{B}_{1,1}^{(2)}, \\ \mathbf{A}_5 &= \mathbf{A}_{1,1} + \mathbf{A}_{1,2}, & \mathbf{B}_5^{(1)} &= \mathbf{B}_{2,2}^{(1)}, & \mathbf{B}_5^{(2)} &= \mathbf{B}_{2,2}^{(2)}, \\ \mathbf{A}_6 &= \mathbf{A}_{2,1} - \mathbf{A}_{1,1}, & \mathbf{B}_6^{(1)} &= \mathbf{B}_{1,1}^{(1)} + \mathbf{B}_{1,2}^{(1)}, & \mathbf{B}_6^{(2)} &= \mathbf{B}_{1,1}^{(2)} + \mathbf{B}_{1,2}^{(2)}, \\ \mathbf{A}_7 &= \mathbf{A}_{1,2} - \mathbf{A}_{2,2}, & \mathbf{B}_7^{(1)} &= \mathbf{B}_{2,1}^{(1)} + \mathbf{B}_{2,2}^{(1)}, & \mathbf{B}_7^{(2)} &= \mathbf{B}_{2,1}^{(2)} + \mathbf{B}_{2,2}^{(2)}. \end{aligned}$$

The desired computation $\mathbf{C}^{(1)}$ in (19) can be recovered from the element-wise product $\{\mathbf{A}_r \mathbf{B}_r^{(1)}\}_{r \in [7]}$ by

$$\begin{aligned}\mathbf{C}_{1,1}^{(1)} &= \mathbf{A}_1 \mathbf{B}_1^{(1)} + \mathbf{A}_4 \mathbf{B}_4^{(1)} - \mathbf{A}_5 \mathbf{B}_5^{(1)} + \mathbf{A}_7 \mathbf{B}_7^{(1)}, \\ \mathbf{C}_{1,2}^{(1)} &= \mathbf{A}_3 \mathbf{B}_3^{(1)} + \mathbf{A}_5 \mathbf{B}_5^{(1)}, \\ \mathbf{C}_{2,1}^{(1)} &= \mathbf{A}_2 \mathbf{B}_2^{(1)} + \mathbf{A}_4 \mathbf{B}_4^{(1)}, \\ \mathbf{C}_{2,2}^{(1)} &= \mathbf{A}_1 \mathbf{B}_1^{(1)} - \mathbf{A}_2 \mathbf{B}_2^{(1)} + \mathbf{A}_3 \mathbf{B}_3^{(1)} + \mathbf{A}_6 \mathbf{B}_6^{(1)}.\end{aligned}$$

Let $\{\beta_r, \alpha_i : r \in [9], i \in [N]\}$ be $N + 9$ distinct elements from \mathbb{F}_q . Further, we know from SMM based on Lagrange codes that, the element-wise product $\{\mathbf{A}_r \mathbf{B}_r^{(1)}\}_{r \in [7]}$ can be obtained by evaluating of the product polynomial $g(x) = f_{\mathbf{A}}(x) \cdot h_{\mathbf{B}}(x)$ at points $x = \beta_1, \dots, \beta_7$, where

$$\begin{aligned}f_{\mathbf{A}}(x) &= \sum_{r=1}^7 \mathbf{A}_r \cdot \prod_{j \in [9] \setminus \{r\}} \frac{x - \beta_j}{\beta_r - \beta_j} \\ &\quad + \mathbf{Z}_8^{\mathbf{A}} \cdot \prod_{j \in [9] \setminus \{8\}} \frac{x - \beta_j}{\beta_8 - \beta_j} + \mathbf{Z}_9^{\mathbf{A}} \cdot \prod_{j \in [9] \setminus \{9\}} \frac{x - \beta_j}{\beta_9 - \beta_j}, \\ h_{\mathbf{B}}(x) &= \sum_{r=1}^7 \mathbf{B}_r^{(1)} \cdot \prod_{j \in [9] \setminus \{r\}} \frac{x - \beta_j}{\beta_r - \beta_j} \\ &\quad + \mathbf{Z}_8^{\mathbf{B}} \cdot \prod_{j \in [9] \setminus \{8\}} \frac{x - \beta_j}{\beta_8 - \beta_j} + \mathbf{Z}_9^{\mathbf{B}} \cdot \prod_{j \in [9] \setminus \{9\}} \frac{x - \beta_j}{\beta_9 - \beta_j}.\end{aligned}$$

Here $\mathbf{Z}_8^{\mathbf{A}}, \mathbf{Z}_9^{\mathbf{A}}$ and $\mathbf{Z}_8^{\mathbf{B}}, \mathbf{Z}_9^{\mathbf{B}}$ are the matrices with corresponding dimensions and will be specified later.

In PSMM, let $\mathbf{Z}_8^{\mathbf{A}}, \mathbf{Z}_9^{\mathbf{A}}$ be random matrices to be ensured security over \mathbb{F}_q , and the master shares $\tilde{\mathbf{A}}_i = f_{\mathbf{A}}(\alpha_i)$ with worker i . Moreover, for any $r \in [7]$, the master also shares the queries $q_r^{(1)}(\alpha_i)$ and $q_r^{(2)}(\alpha_i)$ for the sub-matrices $\mathbf{B}_r^{(1)}$ and $\mathbf{B}_r^{(2)}$, respectively, which are given by

$$\begin{aligned}q_r^{(1)}(\alpha_i) &= \prod_{j \in [9] \setminus \{r\}} \frac{\alpha_i - \beta_j}{\beta_r - \beta_j} \\ &\quad + z_{r,8}^{(1)} \cdot \prod_{j \in [9] \setminus \{8\}} \frac{\alpha_i - \beta_j}{\beta_8 - \beta_j} + z_{r,9}^{(1)} \cdot \prod_{j \in [9] \setminus \{9\}} \frac{\alpha_i - \beta_j}{\beta_9 - \beta_j}, \\ q_r^{(2)}(\alpha_i) &= z_{r,8}^{(2)} \cdot \prod_{j \in [9] \setminus \{8\}} \frac{\alpha_i - \beta_j}{\beta_8 - \beta_j} + z_{r,9}^{(2)} \cdot \prod_{j \in [9] \setminus \{9\}} \frac{\alpha_i - \beta_j}{\beta_9 - \beta_j},\end{aligned}$$

where $z_{r,8}^{(1)}, z_{r,9}^{(1)}$ and $z_{r,8}^{(2)}, z_{r,9}^{(2)}$ are random noises from \mathbb{F}_q . Then worker i encodes the library into

$$\begin{aligned}\tilde{\mathbf{B}}_i &= \sum_{r=1}^7 \mathbf{B}_r^{(1)} q_r^{(1)}(\alpha_i) + \sum_{r=1}^7 \mathbf{B}_r^{(2)} q_r^{(2)}(\alpha_i) \\ &= \sum_{r=1}^7 \mathbf{B}_r^{(1)} \cdot \prod_{j \in [9] \setminus \{r\}} \frac{\alpha_i - \beta_j}{\beta_r - \beta_j} \\ &\quad + \mathbf{Z}_8^{\mathbf{B}} \cdot \prod_{j \in [9] \setminus \{8\}} \frac{\alpha_i - \beta_j}{\beta_8 - \beta_j} + \mathbf{Z}_9^{\mathbf{B}} \cdot \prod_{j \in [9] \setminus \{9\}} \frac{\alpha_i - \beta_j}{\beta_9 - \beta_j},\end{aligned}$$

where we set $\mathbf{Z}_k^{\mathbf{B}} = \sum_{r=1}^7 \mathbf{B}_r^{(1)} z_{r,k}^{(1)} + \sum_{r=1}^7 \mathbf{B}_r^{(2)} z_{r,k}^{(2)}$ for any $k = 8, 9$. Next, worker i computes $\tilde{\mathbf{A}}_i \tilde{\mathbf{B}}_i$ as a response, which is the evaluation of $g(x) = f_{\mathbf{A}}(x) \cdot h_{\mathbf{B}}(x)$ at point $x = \alpha_i$. Hence, the master can interpolate the product $g(x)$ from any

$K = \deg(g(x)) + 1 = 17$ responses, and then recovers $\mathbf{C}^{(1)} = \mathbf{A} \mathbf{B}^{(1)}$.

The general construction is described as follows. Similar to (11) and (12), the master and each worker converts the matrices \mathbf{A} and $\mathbf{B}^{(v)}$ (17) into a batch of sub-matrices of length R , respectively, as shown below.

$$\mathbf{A}_r = \sum_{k=1}^m \sum_{\ell=1}^p a_{r,k,\ell} \mathbf{A}_{k,\ell}, \quad \forall r \in [R], \quad (31)$$

$$\mathbf{B}_r^{(v)} = \sum_{\ell=1}^p \sum_{j=1}^n b_{r,\ell,j} \mathbf{B}_{\ell,j}^{(v)}, \quad \forall r \in [R], v \in [V]. \quad (32)$$

By (10), the master can recover the desired computation $\mathbf{A} \mathbf{B}^{(\theta)}$ if it is able to obtain the element-wise product $\{\mathbf{A}_r \mathbf{B}_r^{(\theta)} : r \in [R]\}$ of the two batches of sub-matrices $(\mathbf{A}_1, \dots, \mathbf{A}_R)$ and $(\mathbf{B}_1^{(\theta)}, \dots, \mathbf{B}_R^{(\theta)})$.

Let $\{\beta_r, \alpha_i : r \in [R+T], i \in [N]\}$ be $R+T+N$ pairwise distinct elements from \mathbb{F}_q . To complete the computation, the master employs the encoding function defined in (15) to encode the batch of sub-matrices $(\mathbf{A}_1, \dots, \mathbf{A}_R)$ as

$$\begin{aligned}f_{\mathbf{A}}(x) &= \sum_{r=1}^R \mathbf{A}_r \cdot \prod_{j \in [R+T] \setminus \{r\}} \frac{x - \beta_j}{\beta_r - \beta_j} \\ &\quad + \sum_{k=R+1}^{R+T} \mathbf{Z}_k^{\mathbf{A}} \cdot \prod_{j \in [R+T] \setminus \{k\}} \frac{x - \beta_j}{\beta_k - \beta_j}, \quad (33)\end{aligned}$$

where $\mathbf{Z}_{R+1}^{\mathbf{A}}, \dots, \mathbf{Z}_{R+T}^{\mathbf{A}}$ are random matrices over \mathbb{F}_q with the same dimension as \mathbf{A}_r .

To keep the index θ private, let $\{z_{r,k}^{(v)} : k \in [R+1 : R+T], r \in [R], v \in [V]\}$ be TRV independently and uniformly random noises from \mathbb{F}_q . Then, given any $v \in [V], r \in [R]$, based on the structure of the encoding function defined in (16), the master constructs the query polynomial $q_r^{(v)}(x)$ as

$$\begin{aligned}q_r^{(v)}(x) &= \sum_{k=R+1}^{R+T} z_{r,k}^{(v)} \cdot \prod_{j \in [R+T] \setminus \{k\}} \frac{x - \beta_j}{\beta_k - \beta_j} \\ &\quad + \begin{cases} \prod_{j \in [R+T] \setminus \{r\}} \frac{x - \beta_j}{\beta_r - \beta_j}, & \text{if } v = \theta \\ 0, & \text{if } v \neq \theta \end{cases}. \quad (34)\end{aligned}$$

Then the master evaluates $f_{\mathbf{A}}(x)$ and $\{q_r^{(v)}(x) : r \in [R], v \in [V]\}$ at point $x = \alpha_i$, and sends them to worker i , i.e.,

$$\tilde{\mathbf{A}}_i = f_{\mathbf{A}}(\alpha_i), \quad (35)$$

$$\mathcal{Q}_i^{(\theta)} = \{q_r^{(v)}(\alpha_i) : r \in [R], v \in [V]\}. \quad (36)$$

Upon the received query, worker i encodes the matrices $\mathbf{B}^{([V])}$ into

$$\tilde{\mathbf{B}}_i = \sum_{v=1}^V \sum_{r=1}^R \mathbf{B}_r^{(v)} \cdot q_r^{(v)}(\alpha_i). \quad (37)$$

By (34), we can denote the encoding function $h_{\mathbf{B}}(x)$ of matrices $\mathbf{B}^{([V])}$ by

$$h_{\mathbf{B}}(x) = \sum_{v=1}^V \sum_{r=1}^R \mathbf{B}_r^{(v)} \cdot q_r^{(v)}(x)$$

$$= \sum_{r=1}^R \mathbf{B}_r^{(\theta)} \cdot \prod_{j \in [R+T] \setminus \{r\}} \frac{x - \beta_j}{\beta_r - \beta_j} + \sum_{k=R+1}^{R+T} \mathbf{z}_k^{\mathbf{B}} \cdot \prod_{j \in [R+T] \setminus \{k\}} \frac{x - \beta_j}{\beta_k - \beta_j}, \quad (38)$$

where

$$\mathbf{z}_k^{\mathbf{B}} = \sum_{v=1}^V \sum_{r=1}^R \mathbf{B}_r^{(v)} \cdot z_{r,k}^{(v)}.$$

Note from (38) that, the function $h_{\mathbf{B}}(x)$ has the identical structure as $h_L(x)$ in (16), which aligns the batch of desired sub-matrices $\{\mathbf{B}_r^{(\theta)}\}_{r \in [R]}$ along the R dimensions corresponding to $\{\prod_{j \in [R+T] \setminus \{r\}} \frac{x - \beta_j}{\beta_r - \beta_j}\}_{r \in [R]}$ and the interference from the matrices $\mathbf{B}^{(V)}$ is aligned along the T dimensions corresponding to $\{\prod_{j \in [R+T] \setminus \{k\}} \frac{x - \beta_j}{\beta_k - \beta_j}\}_{k \in [R+1:R+T]}$.

Then worker i computes $\mathbf{Y}_i^{(\theta)} = \tilde{\mathbf{A}}_i \tilde{\mathbf{B}}_i$, which is the evaluation of the product polynomial $g(x) = f_{\mathbf{A}}(x) \cdot h_{\mathbf{B}}(x)$ at point $x = \alpha_i$. Thus, the master can interpolate the polynomial $g(x)$ from the responses of any $K = \deg(g(x)) + 1 = 2R + 2T - 1$ workers, and then evaluates $g(x)$ at points $x = \beta_1, \dots, \beta_R$ to obtain the desired element-wise product $\{\mathbf{A}_r \mathbf{B}_r^{(\theta)} : r \in [R]\}$.

C. Security, Privacy, Communication Cost and Computation Complexity for PSMM

In this subsection, we prove the security and privacy of the two PSMM strategies above, analyse their communication cost and computation complexities, and compare their performance.

1) *Security and Privacy*: In the proposed PSMM strategy based on polynomial codes, the encoding matrices $\tilde{\mathbf{A}}_i$ (24) and the queries $\mathcal{Q}_i^{(\theta)}$ (25) sent to workers are generated by evaluating the encoding polynomial $f_{\mathbf{A}}(x)$ of matrix \mathbf{A} and the query polynomials $\{q_{\ell,j}^{(v)}(x)\}_{\ell \in [p], j \in [n], v \in [V]}$ at distinct points, respectively. Here the encoding polynomial $f_{\mathbf{A}}(x)$ (22) (resp. each of query polynomial $q_{\ell,j}^{(v)}(x)$ (23)) is constructed by employing T independent and uniform random noises to mask the confidential matrix \mathbf{A} (resp. the interested index θ), which ensures that the data sent to any T workers are secure (resp. private). The security and privacy of the PSMM strategy based on Lagrange codes follows from similar argument. Their formal proofs are presented in Appendix-A.

2) *Communication Cost*: In the two PSMM strategies, the master sends an encoding sub-matrix with the same dimension of $\frac{\lambda}{m} \times \frac{\omega}{p}$ to each worker by (24) and (35), and downloads a matrix with the same dimension of $\frac{\lambda}{m} \times \frac{\gamma}{n}$ from each of responsive workers. Thus, by (3), the two strategies achieve the same upload cost $P_u = \frac{N \times \frac{\lambda}{m} \times \frac{\omega}{p}}{\lambda \times \omega} = \frac{N}{mp}$ and the download cost $P_d = \frac{K \times \frac{\lambda}{m} \times \frac{\gamma}{n}}{\lambda \times \gamma} = \frac{K}{mn}$, where $K = \max\{a_{k,\ell}, c_t : k \in [m], \ell \in [p], t \in [T]\} + \max\{b_{\ell,j}, d_t : \ell \in [p], j \in [n], t \in [T]\} + 1$ and $K = 2R + 2T - 1$ for the PSMM strategies based on polynomial codes and Lagrange codes, respectively.

3) *Computation Complexity*: In the PSMM strategy based on polynomial codes, the encoding process for matrix \mathbf{A} can be viewed as evaluating a polynomial of degree less than N at N points for $\frac{\lambda\omega}{mp}$ times by (22) and (24), and decoding

requires interpolating a $(K-1)$ -th degree polynomial for $\frac{\lambda\gamma}{mn}$ times, where $K = \max\{a_{k,\ell}, c_t : k \in [m], \ell \in [p], t \in [T]\} + \max\{b_{\ell,j}, d_t : \ell \in [p], j \in [n], t \in [T]\} + 1$. It is well known [51] that the evaluation of a k -th degree polynomial at $k+1$ arbitrary points can be done in $O(k(\log k)^2 \log \log k)$ arithmetic operations, and consequently, its dual problem, interpolation of a k -th degree polynomial from $k+1$ arbitrary points can be performed in the same arithmetic operations $O(k(\log k)^2 \log \log k)$. Thus, encoding and decoding achieve the complexities $O(\frac{\lambda\omega N (\log N)^2 \log \log N}{mp})$ and $O(\frac{\lambda\gamma K (\log K)^2 \log \log K}{mn})$, respectively. The complexity at each worker includes generating a linear combination of Vpn sub-matrices with dimension $\frac{\omega\gamma}{np}$ (26), and multiplying two coded sub-matrices with sizes $\frac{\lambda}{m} \times \frac{\omega}{p}$ and $\frac{\omega}{p} \times \frac{\gamma}{n}$, which requires a complexity of $O(V\omega\gamma + \frac{\lambda\omega\gamma}{mpn})$ at most.

In the PSMM strategy based on Lagrange codes, the encoding process for matrix \mathbf{A} includes generating a bath of sub-matrices by taking a linear combination of mp partitioning sub-matrices with dimension $\frac{\lambda\omega}{mp}$ for R times (31), and encoding the batch of sub-matrices by evaluating a polynomial of degree $R+T-1 < N$ at N points for $\frac{\lambda\omega}{mp}$ times by (33) and (35), which achieves the complexity $O(R\lambda\omega + \frac{\lambda\omega N (\log N)^2 \log \log N}{mp})$. The complexity at each worker consists of generating another bath of sub-matrices by taking a linear combination of pn partitioning sub-matrices with dimension $\frac{\omega\gamma}{np}$ for VR times (32), computing a linear combination of VR sub-matrices with dimension $\frac{\omega\gamma}{np}$ (37), and multiplying two coded sub-matrices with sizes $\frac{\lambda}{m} \times \frac{\omega}{p}$ and $\frac{\omega}{p} \times \frac{\gamma}{n}$, which requires a complexity of $O(VR\omega\gamma + \frac{\lambda\omega\gamma}{mpn})$. Decoding requires interpolating of a $(K-1)$ -th degree polynomial for $\frac{\lambda\gamma}{mn}$ times, then evaluating the polynomial at $R < K$ points for $\frac{\lambda\gamma}{mn}$ times, and finally computing the linear combinations of R sub-matrices with dimension $\frac{\lambda\gamma}{mn}$ for mn times (10), which achieves the complexity $O(\frac{\lambda\gamma K (\log K)^2 \log \log K}{mn} + R\lambda\gamma)$, where $K = 2R + 2T - 1$.

4) *Performance Comparison Between the Proposed PSMM Strategies*: We summarize the performance of the two proposed PSMM strategies in Table II. Recall from Remark 2 that which one of the two PSMM strategies achieves a smaller recovery threshold depends on the value of the security parameter T . We observe from Table II that, regardless of the value of T , the PSMM strategy based on polynomial codes outperforms the strategy based on Lagrange codes in terms of encoding complexity and worker computation complexity, with the upload cost being identical. When $K_P \leq K_L$ for some values of the parameter T , the PSMM strategy based on polynomial codes achieves a smaller recovery threshold, download cost, and decoding complexity, and otherwise (i.e., when $K_P > K_L$) the one based on Lagrange codes achieves a smaller recovery threshold and download cost. In the former case of $K_P \leq K_L$, the strategy based on polynomial codes is preferable to facilitate a faster execution of PSMM. However, in the latter case of $K_P > K_L$, one should choose which strategy to implement according to the system resources including the computation and communication capabilities of the master and the workers.

TABLE II
PERFORMANCE OF THE PROPOSED PSMM STRATEGIES.

	PSMM based on Polynomial codes	PSMM based on Lagrange codes
Recovery Threshold	$K_P = \max\{a_{k,\ell}, c_t : k \in [m], \ell \in [p], t \in [T]\} + \max\{b_{\ell,j}, d_t : \ell \in [p], j \in [n], t \in [T]\} + 1$	$K_L = 2R + 2T - 1$
Upload and Download (P_u, P_d)	$\left(\frac{N}{mp}, \frac{K_P}{mn}\right)$	$\left(\frac{N}{mp}, \frac{K_L}{mn}\right)$
Encoding Complexity C_A	$O\left(\frac{\lambda\omega N(\log N)^2 \log \log N}{mp}\right)$	$O\left(R\lambda\omega + \frac{\lambda\omega N(\log N)^2 \log \log N}{mp}\right)$
Worker Computation C_w	$O(V\omega\gamma + \frac{\lambda\omega\gamma}{mpn})$	$O(VR\omega\gamma + \frac{\lambda\omega\gamma}{mpn})$
Decoding Complexity C_d	$O\left(\frac{\lambda\gamma K_P(\log K_P)^2 \log \log K_P}{mn}\right)$	$O\left(\frac{\lambda\gamma K_L(\log K_L)^2 \log \log K_L}{mn} + R\lambda\gamma\right)$

Here, K_P can take the value of $\min\{(m+1)(np+T)-1, (n+1)(mp+T)-1, 2mpn+2T-1\}$ by Corollary 1, and R denotes any upper construction of bilinear complexity.

VI. COMPUTATION STRATEGIES FOR FULLY PRIVATE MATRIX MULTIPLICATION

In this section, we present the FPMM strategies based on polynomial codes and Lagrange codes for proving Theorems 3 and 4, respectively, and then analyse their privacy, communication cost and computation complexities.

As illustrated in Fig. 2, the goal of the master in FPMM is to compute the product $\mathbf{A}^{(\theta_1)}\mathbf{B}^{(\theta_2)}$ for any $\theta_1 \in [U]$ and $\theta_2 \in [V]$, while keeping the indices of the desired product θ_1 and θ_2 private from any T colluding workers. Consider arbitrary partitioning parameters m, p, n , the matrices $\mathbf{A}^{(u)}$ and $\mathbf{B}^{(v)}$ are divided into $m \times p$ and $p \times n$ equal-size sub-matrices, respectively, i.e., for all $u \in [U], v \in [V]$,

$$\mathbf{A}^{(u)} = \begin{bmatrix} \mathbf{A}_{1,1}^{(u)} & \cdots & \mathbf{A}_{1,p}^{(u)} \\ \vdots & \ddots & \vdots \\ \mathbf{A}_{m,1}^{(u)} & \cdots & \mathbf{A}_{m,p}^{(u)} \end{bmatrix}, \quad \mathbf{B}^{(v)} = \begin{bmatrix} \mathbf{B}_{1,1}^{(v)} & \cdots & \mathbf{B}_{1,n}^{(v)} \\ \vdots & \ddots & \vdots \\ \mathbf{B}_{p,1}^{(v)} & \cdots & \mathbf{B}_{p,n}^{(v)} \end{bmatrix}, \quad (39)$$

where $\mathbf{A}_{k,\ell}^{(u)} \in \mathbb{F}_q^{\frac{\lambda}{m} \times \frac{\omega}{p}}$ for any $k \in [m], \ell \in [p]$, and $\mathbf{B}_{\ell,j}^{(v)} \in \mathbb{F}_q^{\frac{\omega}{p} \times \frac{\gamma}{n}}$ for any $\ell \in [p], j \in [n]$. Thus, the desired product $\mathbf{C}^{(\theta_1, \theta_2)} = \mathbf{A}^{(\theta_1)}\mathbf{B}^{(\theta_2)}$ is given by

$$\mathbf{C}^{(\theta_1, \theta_2)} = \mathbf{A}^{(\theta_1)}\mathbf{B}^{(\theta_2)} = \begin{bmatrix} \mathbf{C}_{1,1}^{(\theta_1, \theta_2)} & \cdots & \mathbf{C}_{1,n}^{(\theta_1, \theta_2)} \\ \vdots & \ddots & \vdots \\ \mathbf{C}_{m,1}^{(\theta_1, \theta_2)} & \cdots & \mathbf{C}_{m,n}^{(\theta_1, \theta_2)} \end{bmatrix}$$

with $\mathbf{C}_{k,j}^{(\theta_1, \theta_2)} = \sum_{\ell=1}^p \mathbf{A}_{k,\ell}^{(\theta_1)}\mathbf{B}_{\ell,j}^{(\theta_2)}$ for any $k \in [m], j \in [n]$.

A. FPMM Strategy Based on Polynomial Codes

We start with proving Theorem 3. Similar to PSMM strategy based on polynomial codes, we show that any SMM strategy based on polynomial codes can be exploited to construct the FPMM strategy with same recovery threshold.

Let the positive integers $\{a_{k,\ell}, b_{\ell,j}, c_t, d_t : k \in [m], \ell \in [p], j \in [n], t \in [T]\}$ satisfying C1-C2 be the parameters of the SMM strategy based on polynomial codes. For any $t \in [T]$, let $\mathbf{Z}_t^{\mathbf{A}}$ and $\mathbf{Z}_t^{\mathbf{B}}$ be arbitrary matrices over \mathbb{F}_q with the same dimensions as $\mathbf{A}_{k,\ell}^{(\theta_1)}$ and $\mathbf{B}_{\ell,j}^{(\theta_2)}$ respectively, and their forms will be specified later. Note from Section III-A that, the desired computation $\mathbf{C}^{(\theta_1, \theta_2)}$ can be completed if one recovers the product polynomial $g(x) = f_{\mathbf{A}}(x) \cdot h_{\mathbf{B}}(x)$, where

$$f_{\mathbf{A}}(x) = \sum_{k=1}^m \sum_{\ell=1}^p \mathbf{A}_{k,\ell}^{(\theta_1)} x^{a_{k,\ell}} + \sum_{t=1}^T \mathbf{Z}_t^{\mathbf{A}} x^{c_t}, \quad (40)$$

$$h_{\mathbf{B}}(x) = \sum_{\ell=1}^p \sum_{j=1}^n \mathbf{B}_{\ell,j}^{(\theta_2)} x^{b_{\ell,j}} + \sum_{t=1}^T \mathbf{Z}_t^{\mathbf{B}} x^{d_t}. \quad (41)$$

To keep the index θ_1 private, let $\{\tilde{z}_{k,\ell,t}^{(u)} : t \in [T], k \in [m], \ell \in [p], u \in [U]\}$ be $UTmp$ random noises chosen independently and uniformly from \mathbb{F}_q . Then for each partitioning sub-matrix $\mathbf{A}_{k,\ell}^{(u)}$ in $\mathbf{A}^{([U])}$ for any $k \in [m], \ell \in [p], u \in [U]$, the master constructs the query polynomial $\rho_{k,\ell}^{(u)}(x)$ based on the structure of the encoding function in (40), which is given by

$$\rho_{k,\ell}^{(u)}(x) = \sum_{t=1}^T \tilde{z}_{k,\ell,t}^{(u)} \cdot x^{c_t} + \begin{cases} x^{a_{k,\ell}}, & \text{if } u = \theta_1 \\ 0, & \text{if } u \neq \theta_1 \end{cases}. \quad (42)$$

Similar to (23), based on the structure of the encoding function in (41), the master also constructs the query polynomial $q_{\ell,j}^{(v)}(x)$ for each partitioning sub-matrix $\mathbf{B}_{\ell,j}^{(v)}$ in $\mathbf{B}^{([V])}$ for any $\ell \in [p], j \in [n], v \in [V]$, given by

$$q_{\ell,j}^{(v)}(x) = \sum_{t=1}^T \tilde{z}_{\ell,j,t}^{(v)} \cdot x^{d_t} + \begin{cases} x^{b_{\ell,j}}, & \text{if } v = \theta_2 \\ 0, & \text{if } v \neq \theta_2 \end{cases}, \quad (43)$$

where $\tilde{z}_{\ell,j,t}^{(v)}$ is uniformly random noise from \mathbb{F}_q .

Let $\alpha_1, \alpha_2, \dots, \alpha_N$ be the pairwise distinct non-zero elements in \mathbb{F}_q . The master shares the following evaluations with worker i :

$$\mathcal{Q}_i^{(\theta_1)} = \{\rho_{k,\ell}^{(u)}(\alpha_i) : k \in [m], \ell \in [p], u \in [U]\}, \quad (44)$$

$$\mathcal{Q}_i^{(\theta_2)} = \{q_{\ell,j}^{(v)}(\alpha_i) : \ell \in [p], j \in [n], v \in [V]\}. \quad (45)$$

After that, worker i encodes the matrices $\mathbf{A}^{([U])}$ and $\mathbf{B}^{([V])}$ (39) into

$$\tilde{\mathbf{A}}_i = \sum_{u=1}^U \sum_{k=1}^m \sum_{\ell=1}^p \mathbf{A}_{k,\ell}^{(u)} \cdot \rho_{k,\ell}^{(u)}(\alpha_i), \quad (46)$$

$$\tilde{\mathbf{B}}_i = \sum_{v=1}^V \sum_{\ell=1}^p \sum_{j=1}^n \mathbf{B}_{\ell,j}^{(v)} \cdot q_{\ell,j}^{(v)}(\alpha_i). \quad (47)$$

By (40)–(43), we have

$$\begin{aligned} \sum_{u=1}^U \sum_{k=1}^m \sum_{\ell=1}^p \mathbf{A}_{k,\ell}^{(u)} \cdot \rho_{k,\ell}^{(u)}(x) \\ = \sum_{k=1}^m \sum_{\ell=1}^p \mathbf{A}_{k,\ell}^{(\theta_1)} x^{a_{k,\ell}} + \sum_{t=1}^T \mathbf{Z}_t^{\mathbf{A}} x^{c_t} = f_{\mathbf{A}}(x), \end{aligned} \quad (48)$$

$$\begin{aligned} & \sum_{v=1}^V \sum_{\ell=1}^p \sum_{j=1}^n \mathbf{B}_{\ell,j}^{(v)} \cdot q_{\ell,j}^{(v)}(x) \\ &= \sum_{\ell=1}^p \sum_{j=1}^n \mathbf{B}_{\ell,j}^{(\theta)} x^{b_{\ell,j}} + \sum_{t=1}^T \mathbf{Z}_t^{\mathbf{B}} x^{d_t} = h_{\mathbf{B}}(x), \end{aligned} \quad (49)$$

where we set

$$\begin{aligned} \mathbf{Z}_t^{\mathbf{A}} &= \sum_{u=1}^U \sum_{k=1}^m \sum_{\ell=1}^p \mathbf{A}_{k,\ell}^{(u)} \tilde{z}_{k,\ell,t}^{(u)}, \quad \forall t \in [T], \\ \mathbf{Z}_t^{\mathbf{B}} &= \sum_{v=1}^V \sum_{\ell=1}^p \sum_{j=1}^n \mathbf{B}_{\ell,j}^{(v)} z_{\ell,j,t}^{(v)}, \quad \forall t \in [T], \end{aligned}$$

which are independent of workers and thus can be viewed as constant terms.

Then each worker $i \in [N]$ computes the product $\mathbf{Y}_i^{(\theta_1, \theta_2)} = \tilde{\mathbf{A}}_i \tilde{\mathbf{B}}_i$ as a response for the master, which is equivalent to evaluating the product polynomial $g(x) = f_{\mathbf{A}}(x) \cdot h_{\mathbf{B}}(x)$ at point $x = \alpha_i$ by (46)–(49). Thus, the master can interpolate the product $g(x)$ from the responses of any $K = \max\{a_{k,\ell}, c_t : k \in [m], \ell \in [p], t \in [T]\} + \max\{b_{\ell,j}, d_t : \ell \in [p], j \in [n], t \in [T]\} + 1$ workers and then recovers the desired computation $\mathbf{C}^{(\theta_1, \theta_2)}$.

B. FPMM Strategy Based on Lagrange Codes

We now present the FPMM strategy based on Lagrange codes for proving Theorem 4. Let $a = (a_{r,k,\ell}), b = (b_{r,\ell,j}), c = (c_{r,k,j})$ be any upper bound construction with rank R for bilinear complexity. Each worker first converts the matrices $\mathbf{A}^{(u)}$ and $\mathbf{B}^{(v)}$ (39) into a batch of sub-matrices of length R , respectively:

$$\mathbf{A}_r^{(u)} = \sum_{k=1}^m \sum_{\ell=1}^p a_{r,k,\ell} \mathbf{A}_{k,\ell}^{(u)}, \quad \forall r \in [R], u \in [U], \quad (50)$$

$$\mathbf{B}_r^{(v)} = \sum_{\ell=1}^p \sum_{j=1}^n b_{r,\ell,j} \mathbf{B}_{\ell,j}^{(v)}, \quad \forall r \in [R], v \in [V]. \quad (51)$$

Let $\{\beta_r, \alpha_i : r \in [R+T], i \in [N]\}$ be $R+T+N$ distinct elements from \mathbb{F}_q . Denote the polynomial functions of $\mathbf{A}^{(\theta_1)}$ and $\mathbf{B}^{(\theta_2)}$ by

$$\begin{aligned} f_{\mathbf{A}}(x) &= \sum_{r=1}^R \mathbf{A}_r^{(\theta_1)} \cdot \prod_{j \in [R+T] \setminus \{r\}} \frac{x - \beta_j}{\beta_r - \beta_j} \\ &\quad + \sum_{k=R+1}^{R+T} \mathbf{Z}_k^{\mathbf{A}} \cdot \prod_{j \in [R+T] \setminus \{k\}} \frac{x - \beta_j}{\beta_k - \beta_j}, \end{aligned} \quad (52)$$

$$\begin{aligned} h_{\mathbf{B}}(x) &= \sum_{r=1}^R \mathbf{B}_r^{(\theta_2)} \cdot \prod_{j \in [R+T] \setminus \{r\}} \frac{x - \beta_j}{\beta_r - \beta_j} \\ &\quad + \sum_{k=R+1}^{R+T} \mathbf{Z}_k^{\mathbf{B}} \cdot \prod_{j \in [R+T] \setminus \{k\}} \frac{x - \beta_j}{\beta_k - \beta_j}, \end{aligned} \quad (53)$$

where $\mathbf{Z}_{R+1}^{\mathbf{A}}, \dots, \mathbf{Z}_{R+T}^{\mathbf{A}}$ and $\mathbf{Z}_{R+1}^{\mathbf{B}}, \dots, \mathbf{Z}_{R+T}^{\mathbf{B}}$ are arbitrary matrices over \mathbb{F}_q with the same dimensions as $\mathbf{A}_r^{(\theta_1)}$ and $\mathbf{B}_r^{(\theta_2)}$ respectively, and will be explained later. We know from Section III-B that, one can recover the desired computation

$\mathbf{C}^{(\theta_1, \theta_2)} = \mathbf{A}^{(\theta_1)} \mathbf{B}^{(\theta_2)}$ by interpolating the product polynomial $g(x) = f_{\mathbf{A}}(x) \cdot h_{\mathbf{B}}(x)$.

To keep the indices θ_1 and θ_2 private, the master constructs the query polynomials $\rho_r^{(u)}(x)$ and $q_r^{(v)}(x)$ by exploiting the structure of the encoding functions in (52) and (53), respectively, for all $r \in [R], u \in [U], v \in [V]$, as follows.

$$\begin{aligned} \rho_r^{(u)}(x) &= \sum_{k=R+1}^{R+T} \tilde{z}_{r,k}^{(u)} \cdot \prod_{j \in [R+T] \setminus \{k\}} \frac{x - \beta_j}{\beta_k - \beta_j} \\ &\quad + \begin{cases} \prod_{j \in [R+T] \setminus \{r\}} \frac{x - \beta_j}{\beta_r - \beta_j}, & \text{if } u = \theta_1 \\ 0, & \text{if } u \neq \theta_1 \end{cases}, \end{aligned} \quad (54)$$

$$\begin{aligned} q_r^{(v)}(x) &= \sum_{k=R+1}^{R+T} z_{r,k}^{(v)} \cdot \prod_{j \in [R+T] \setminus \{k\}} \frac{x - \beta_j}{\beta_k - \beta_j} \\ &\quad + \begin{cases} \prod_{j \in [R+T] \setminus \{r\}} \frac{x - \beta_j}{\beta_r - \beta_j}, & \text{if } v = \theta_2 \\ 0, & \text{if } v \neq \theta_2 \end{cases}, \end{aligned} \quad (55)$$

where $\tilde{z}_{r,k}^{(u)}$ and $z_{r,k}^{(v)}$ are independently and uniformly random noises from \mathbb{F}_q .

Then the master evaluates the query polynomials and sends them to worker i , i.e.,

$$\mathcal{Q}_i^{(\theta_1)} = \{\rho_r^{(u)}(\alpha_i) : r \in [R], u \in [U]\}, \quad (56)$$

$$\mathcal{Q}_i^{(\theta_2)} = \{q_r^{(v)}(\alpha_i) : r \in [R], v \in [V]\}. \quad (57)$$

According to the received queries, worker i encodes its matrices $\mathbf{A}^{([U])}$ and $\mathbf{B}^{([V])}$ into

$$\tilde{\mathbf{A}}_i = \sum_{u=1}^U \sum_{r=1}^R \mathbf{A}_r^{(u)} \cdot \rho_r^{(u)}(\alpha_i), \quad (58)$$

$$\tilde{\mathbf{B}}_i = \sum_{v=1}^V \sum_{r=1}^R \mathbf{B}_r^{(v)} \cdot q_r^{(v)}(\alpha_i). \quad (59)$$

By (52)–(55), we have

$$\begin{aligned} \sum_{u=1}^U \sum_{r=1}^R \mathbf{A}_r^{(u)} \cdot \rho_r^{(u)}(x) &= \sum_{r=1}^R \mathbf{A}_r^{(\theta_1)} \cdot \prod_{j \in [R+T] \setminus \{r\}} \frac{x - \beta_j}{\beta_r - \beta_j} \\ &\quad + \sum_{k=R+1}^{R+T} \mathbf{Z}_k^{\mathbf{A}} \cdot \prod_{j \in [R+T] \setminus \{k\}} \frac{x - \beta_j}{\beta_k - \beta_j} = f_{\mathbf{A}}(x), \\ \sum_{v=1}^V \sum_{r=1}^R \mathbf{B}_r^{(v)} \cdot q_r^{(v)}(x) &= \sum_{r=1}^R \mathbf{B}_r^{(\theta_2)} \cdot \prod_{j \in [R+T] \setminus \{r\}} \frac{x - \beta_j}{\beta_r - \beta_j} \\ &\quad + \sum_{k=R+1}^{R+T} \mathbf{Z}_k^{\mathbf{B}} \cdot \prod_{j \in [R+T] \setminus \{k\}} \frac{x - \beta_j}{\beta_k - \beta_j} = h_{\mathbf{B}}(x), \end{aligned}$$

where we set

$$\begin{aligned} \mathbf{Z}_k^{\mathbf{A}} &= \sum_{u=1}^U \sum_{r=1}^R \mathbf{A}_r^{(u)} \cdot \tilde{z}_{r,k}^{(u)}, \quad \forall k \in [R+1 : R+T], \\ \mathbf{Z}_k^{\mathbf{B}} &= \sum_{v=1}^V \sum_{r=1}^R \mathbf{B}_r^{(v)} \cdot z_{r,k}^{(v)}, \quad \forall k \in [R+1 : R+T], \end{aligned}$$

which are constant terms independently of workers. Then, worker i computes $\mathbf{Y}_i^{(\theta_1, \theta_2)} = \tilde{\mathbf{A}}_i \tilde{\mathbf{B}}_i$, which is the evaluate of

the product polynomial $g(x) = f_{\mathbf{A}}(x) \cdot h_{\mathbf{B}}(x)$ at point $x = \alpha_i$. Thus, the master can interpolate $g(x)$ from the responses of any $K = 2R + 2T - 1$ workers, and then obtains the desired product $\mathbf{C}^{(\theta_1, \theta_2)} = \mathbf{A}^{(\theta_1)} \mathbf{B}^{(\theta_2)}$.

C. Privacy, Communication Cost and Computation Complexity for FPMM

For the two FPMM strategies above, their privacy, communication cost, computation complexities and comparisons follow from the similar discussion to the PSMM strategies in Section V-C. We briefly outline as follows.

1) *Privacy*: In the two FPMM strategies, the queries $\mathcal{Q}_i^{(\theta_1)}$ and $\mathcal{Q}_i^{(\theta_2)}$ sent to workers are generated by evaluating the query polynomials $\{\rho_{k,\ell}^{(u)}(x)\}_{k \in [m], \ell \in [p], u \in [U]}$ and $\{q_{\ell,j}^{(v)}(x)\}_{\ell \in [p], j \in [n], v \in [V]}$ (or $\{\rho_r^{(u)}(\alpha_i)\}_{r \in [R], u \in [U]}$ and $\{q_r^{(v)}(\alpha_i)\}_{r \in [R], v \in [V]}$) at distinct points, where each of query polynomials is constructed by employing T independent and uniform random noises to mask interested index, which ensures the privacy of the queries sent to any T workers. Their formal proofs are given in Appendix-B.

2) *Communication Cost*: In the two strategies, the master downloads a matrix with the same dimension of $\frac{\lambda}{m} \times \frac{\gamma}{n}$ from each of responsive workers. Thus, the two strategies achieve the download cost $P_d = \frac{K \times \frac{\lambda}{m} \times \frac{\gamma}{n}}{\lambda \times \gamma} = \frac{K}{mn}$, where $K = \max\{a_{k,\ell}, c_t : k \in [m], \ell \in [p], t \in [T]\} + \max\{b_{\ell,j}, d_t : \ell \in [p], j \in [n], t \in [T]\} + 1$ and $K = 2R + 2T - 1$ for the FPMM strategies based on polynomial codes and Lagrange codes, respectively.

3) *Computation Complexity*: In the FPMM strategy based on polynomial codes, the complexity at each worker includes encoding the matrices $\mathbf{A}^{([U])}$ by taking a linear combination of Ump sub-matrices with dimension $\frac{\lambda\omega}{mp}$ (46), encoding the matrices $\mathbf{B}^{([V])}$ by taking a linear combination of Vpn sub-matrices with dimension $\frac{\omega\gamma}{np}$ (47), and multiplying the two coded sub-matrices with sizes $\frac{\lambda}{m} \times \frac{\omega}{p}$ and $\frac{\omega}{p} \times \frac{\gamma}{n}$, which requires a complexity of $O(U\lambda\omega + V\omega\gamma + \frac{\lambda\omega\gamma}{mpn})$ at most. Decoding requires interpolating a $(K-1)$ -th degree polynomial for $\frac{\lambda\gamma}{mn}$ times, which achieves the complexity $O(\frac{\lambda\gamma K(\log K)^2 \log \log K}{mn})$, where $K = \max\{a_{k,\ell}, c_t : k \in [m], \ell \in [p], t \in [T]\} + \max\{b_{\ell,j}, d_t : \ell \in [p], j \in [n], t \in [T]\} + 1$.

In the FPMM strategy based on Lagrange codes, the complexity at each worker consists of generating the two batches of sub-matrices $(\mathbf{A}_1^{(u)}, \dots, \mathbf{A}_R^{(u)}), u \in [U]$ and $(\mathbf{B}_R^{(v)}, \dots, \mathbf{B}_1^{(v)}), v \in [V]$ by (50) and (51), encoding the two batches of sub-matrices into $\tilde{\mathbf{A}}_i$ and $\tilde{\mathbf{B}}_i$ by (58)-(59), and multiplying the two coded sub-matrices $\tilde{\mathbf{A}}_i$ and $\tilde{\mathbf{B}}_i$, which achieves the complexity $O(UR\lambda\omega + VR\omega\gamma + \frac{\lambda\omega\gamma}{mpn})$. Decoding is identical to the PSMM strategy based on Lagrange codes, and achieves the complexity $O(\frac{\lambda\gamma K(\log K)^2 \log \log K}{mn} + R\lambda\gamma)$, where $K = 2R + 2T - 1$.

4) *Performance Comparison Between the Proposed FPMM Strategies*: The performance of the two FPMM strategies are summarized in Table III. Following a discussion similar to Section V-C4, it is straightforward to obtain from Table III that, the performance of the FPMM strategy based on polynomial codes strictly outperforms the one based on Lagrange

codes when $K_P \leq K_L$ for some values of the parameter T , and otherwise the one based on Lagrange codes achieves a smaller recovery threshold and download cost, but still with a higher computation complexity at each worker.

VII. COMPARISON WITH RELATED WORKS

The most valuable aspect of this paper is that we propose a novel systematic approach to construct efficient computation strategies for private matrix multiplication problems. The key idea is to start with an SMM strategy (polynomial codes-based or Lagrange codes-based), and then carefully design queries at the master such that 1) the interested matrix indices are completely hidden from any T colluding workers, and 2) the response computed from the query and the local data at each worker resembles the response computed in the SMM strategy. Strategies constructed following this approach directly inherit the correctness of matrix multiplication from the underlying SMM strategy, and the original problem is essentially reduced to the problem of designing private queries that are compatible with the chosen SMM strategy, which substantially simplifies the design process for private matrix multiplication strategies. To clearly see the innovations of this approach in perspective, let us compare the strategies constructed following this approach with the previous PSMM strategies [7], [8], [16], [44], [47] and FPMM strategies [16], [48] that are most relevant to our work.

References [7], [8], [44] exploit Polynomial codes (see, e.g., [18], [20]) to solve the PSMM problem without colluding workers (i.e., $T = 1$). While both the prior works [7], [8], [44] and our first proposed PSMM strategy employ Polynomial codes to encode the confidential matrix \mathbf{A} , the main difference lies in how the queries are designed, which accordingly leads to different worker responses and decoding operation. In [7], [8], [44], the queries are designed such that 1) all elements in a query sent to any individual worker have identical distribution, so no information about the interested index θ is leaked; and 2) the query elements corresponding to θ are pairwise distinct across all workers for completing the desired matrix multiplication, whereas the remaining elements are made identical to align interference from undesired matrices. More specifically, in [7], [8], [44], the query sent to worker i is constructed as $\mathcal{Q}_i^{(\theta)} = \{\alpha_1, \dots, \alpha_{\theta-1}, \alpha_{\theta,i}, \alpha_{\theta+1}, \dots, \alpha_V\}$ for any $i \in [N]$, where $\{\alpha_1, \dots, \alpha_{\theta-1}, \alpha_{\theta+1}, \dots, \alpha_V\}$ and $\{\alpha_{\theta,i}\}_{i \in [N]}$ are $N + V - 1$ pairwise distinct points that are selected uniformly i.i.d. from \mathbb{F}_q . It is not clear how one can generalize this query design to the colluding case considered in this paper, while maintaining the privacy requirement. In our proposed strategy, inspired by the specific structure of the polynomial codes utilized to encode the confidential matrix \mathbf{B} in the SMM problem, we design polynomially coded queries (see, e.g., (23)) that facilitate a form of interference alignment, separating the desired and interfering partitioning sub-matrices in the library $\mathcal{L}^{\mathbf{B}}$, such that the local matrix $\tilde{\mathbf{B}}_i$ obtained from the library and the received query has identical structure as the encoding of the matrix \mathbf{B} in SMM, for each worker i , as shown in (28). Consequently, the proposed PSMM strategies achieve the same recovery thresholds as the SMM strategies.

TABLE III
PERFORMANCE OF THE PROPOSED FPMM STRATEGIES.

	FPMM based on Polynomial codes	FPMM based on Lagrange codes
Recovery Threshold	$K_P = \max\{a_{k,\ell}, c_t : k \in [m], \ell \in [p], t \in [T]\} + \max\{b_{\ell,j}, d_t : \ell \in [p], j \in [n], t \in [T]\} + 1$	$K_L = 2R + 2T - 1$
Download cost P_d	$\frac{K_P}{mn}$	$\frac{K_L}{mn}$
Worker Computation C_w	$O(U\lambda\omega + V\omega\gamma + \frac{\lambda\omega\gamma}{mpn})$	$O(UR\lambda\omega + VR\omega\gamma + \frac{\lambda\omega\gamma}{mpn})$
Decoding Complexity C_d	$O(\frac{\lambda\gamma K_P (\log K_P)^2 \log \log K_P}{mn})$	$O(\frac{\lambda\gamma K_L (\log K_L)^2 \log \log K_L}{mn} + R\lambda\gamma)$

Here, K_P can take the value of $\min\{(m+1)(np+T)-1, (n+1)(mp+T)-1, 2mpn+2T-1\}$ by Corollary 1, and R denotes any upper construction of bilinear complexity.

For the case of non-colluding workers with $T = 1$, the best known recovery threshold achieved by PSMM strategies based on polynomial codes is $mpn + mp + n$ [44]. The recovery threshold and download cost of our PSMM strategy based on polynomial codes is superior to that when $m > n$ and $p > 1$ by Corollary 1, with the other performance of upload cost and computation complexity being identical.

The problem of PSMM with T colluding workers was first studied in [47], for the extremely special case of $p = n = 1$, i.e., only matrix \mathbf{A} is horizontally divided into m equal-size sub-matrices as $\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_m$. To complete desired computation, the PSMM strategy based on polynomial codes in [47] shares V encoding versions $\mathbf{A}_i^{(1)}, \mathbf{A}_i^{(2)}, \dots, \mathbf{A}_i^{(V)}$ of matrix \mathbf{A} to each worker i in a security-preserving manner, which are also used as a query to instruct the worker to compute the response $\mathbf{Y}_i^{(\theta)} = \sum_{v=1}^V \mathbf{A}_i^{(v)} \mathbf{B}^{(v)}$ for the master, where $\mathbf{A}_i^{(v)}$ for any $v \in [V]$ is given by

$$\mathbf{A}_i^{(v)} = \sum_{t=1}^T \mathbf{Z}_t^{(v)} \alpha_i^{t-1} + \begin{cases} \sum_{k=1}^m \mathbf{A}_k \alpha_i^{T+k-1}, & \text{if } v = \theta \\ 0, & \text{if } v \neq \theta \end{cases}.$$

Here $\alpha_1, \dots, \alpha_N$ are distinct elements on \mathbb{F}_q and $\{\mathbf{Z}_t^{(v)}\}_{t \in [T], v \in [V]}$ are random noise matrices. However, this approach requires uploading V encoding versions of \mathbf{A} and pairwise multiplying these encoding sub-matrices with all public matrices in the library \mathcal{L}^B for each worker, implying a significantly communication and computation overheads. In our PSMM strategy based on polynomial code, the master shares only one secure encoding version $\tilde{\mathbf{A}}_i$ (24) of \mathbf{A} , and sends a private query to encode the library \mathcal{L}^B into one encoding sub-matrix $\tilde{\mathbf{B}}_i$ (26). The response of each worker is completed by computing the product of the two encoding sub-matrices $\mathbf{Y}_i^{(\theta)} = \tilde{\mathbf{A}}_i \tilde{\mathbf{B}}_i$ (30). For this special case of $p = n = 1$, compared with the PSMM strategy in [47], our proposed strategy reduces upload cost, encoding complexity, and worker computation complexity by a factor of $O(V)$, at the expense of increased recovery threshold by a factor of 2, where V is the number of matrices in the library \mathcal{L}^B and is typically large in current big data era (see detailed comparison in Table IV).

The FPMM problem with T -colluding workers was previously investigated in [48] for the special case of $p = 1$, and a strategy with recovery threshold $(m+1)(n+T) + T - 1$ is constructed based on the idea of Cross Subspace Alignment (CSA) introduced in [43]. In the strategy proposed in [48], the queries sent to worker i are constructed as $\mathcal{Q}_i^{(\theta_1)} = \{\rho_k^{(u)}(\alpha_i) :$

TABLE IV
PERFORMANCE COMPARISON FOR PSMM STRATEGIES BASED ON POLYNOMIAL CODES, FOR THE CASE OF $p = n = 1$, AND $T > 1$ COLLUDING WORKERS.

	Previous PSMM Strategy [47]	Our PSMM Strategy
Recovery Threshold	$K = m + T$	$K' = 2m + 2T - 1$
Upload Cost	$\frac{VN}{m}$	$\frac{N}{m}$
Download Cost	$\frac{K}{m}$	$\frac{K'}{m}$
Encoding Complexity	$O(\frac{V\lambda\omega N (\log N)^2 \log \log N}{m})$	$O(\frac{\lambda\omega N (\log N)^2 \log \log N}{m})$
Worker Computation	$O(\frac{V\lambda\omega\gamma}{m})$	$O(V\omega\gamma + \frac{\lambda\omega\gamma}{m})$
Decoding Complexity	$O(\frac{\lambda\gamma K (\log K)^2 \log \log K}{mn})$	$O(\frac{\lambda\gamma K' (\log K')^2 \log \log K'}{mn})$

$k \in [m], u \in [U]\}$ and $\mathcal{Q}_i^{(\theta_2)} = \{q_j^{(v)}(\alpha_i) : j \in [n], v \in [V]\}$, where $\rho_k^{(u)}(\alpha_i)$ and $q_j^{(v)}(\alpha_i)$ are given by

$$\rho_k^{(u)}(\alpha_i) = \sum_{t=1}^T \tilde{z}_{k,t}^{(u)} \cdot \alpha_i^{t-1} + \begin{cases} \alpha_i^{-(n+T)k}, & \text{if } u = \theta_1 \\ 0, & \text{if } u \neq \theta_1 \end{cases},$$

$$q_j^{(v)}(\alpha_i) = \sum_{t=1}^T \tilde{z}_{j,t}^{(v)} \cdot \alpha_i^{t-1} + \begin{cases} \alpha_i^{-j}, & \text{if } v = \theta_2 \\ 0, & \text{if } v \neq \theta_2 \end{cases}$$

for some evaluation point α_i and random noises $\tilde{z}_{k,t}^{(u)}, \tilde{z}_{j,t}^{(v)}$. In our FPMM strategy based on polynomial codes, similar to PSMM, with the goal of resembling the structure of encoding functions for the matrices \mathbf{A} and \mathbf{B} in SMM strategies, our FPMM strategies design corresponding polynomially coded queries (see, e.g., (42) and (43)) for the libraries \mathcal{L}^A and \mathcal{L}^B , respectively. For this special case of $p = 1$, our strategy based on polynomial codes strictly outperforms that in [48] in terms of recovery threshold and download cost by Corollary 1, while the performance with respect to other measures are identical.

Strategies based on Lagrange codes were first developed in [16] to solve PSMM and FPMM problems without colluding workers. For this special cases of $T = 1$, our proposed strategy based on Lagrange codes achieves identical system performance as that in [16], for both problems of PSMM and FPMM. The query design in our proposed strategy differs significantly from the design in [16]. While the query design in [16] follows the ideas in [7], [8] for the PSMM problem, and is difficult to generalize to the case of colluding workers, following our systematic approach, we design Lagrange coded queries of the private indices θ_1 and θ_2 , such that the computed response at each worker exhibits identical structure of the response computed using the SMM strategy based on Lagrange codes.

VIII. CONCLUSION

In this paper, we focused on designing efficient PSMM and FPMM strategies that minimize the recovery threshold, communication cost and complexity. We showed that, the current SMM strategies based on polynomial codes and Lagrange codes can be used to construct PSMM/FPMM strategies with same recovery threshold, by exploiting the structure inspired by the encoding functions of the SMM strategies to create private queries. This establishes a generic connection between PSMM/FPMM and SMM, and provides a novel systematic approach towards designing PSMM and FPMM strategies. The resulting strategies constructed from this approach improve one or more efficiency metrics including recovery threshold, communication cost and computation complexity, compared with the state of the art, achieving a more flexible tradeoff in optimizing system efficiency.

APPENDIX

In this appendix, we prove the security and/or privacy of the proposed PSMM/FPMM strategies based on polynomial codes and Lagrange codes.

A. Proof of Security and Privacy for PSMM

We start with proving the security and privacy of the proposed PSMM strategy based on polynomial codes.

Security for PSMM Based on Polynomial Codes: Let $\mathcal{T} = \{i_1, \dots, i_T\} \subseteq [N]$ be any T indices of the N workers. Then,

$$\begin{aligned} I(\mathbf{A}; \mathcal{Q}_{\mathcal{T}}^{(\theta)}, \tilde{\mathbf{A}}_{\mathcal{T}}, \mathbf{B}^{([V])}, \mathbf{Y}_{\mathcal{T}}^{(\theta)}) \\ &= I(\mathbf{A}; \tilde{\mathbf{A}}_{\mathcal{T}}) + I(\mathbf{A}; \mathcal{Q}_{\mathcal{T}}^{(\theta)}, \mathbf{B}^{([V])} | \tilde{\mathbf{A}}_{\mathcal{T}}) \\ &\quad + I(\mathbf{A}; \mathbf{Y}_{\mathcal{T}}^{(\theta)} | \tilde{\mathbf{A}}_{\mathcal{T}}, \mathcal{Q}_{\mathcal{T}}^{(\theta)}, \mathbf{B}^{([V])}) \\ &\stackrel{(a)}{=} I(\mathbf{A}; \tilde{\mathbf{A}}_{\mathcal{T}}) \\ &\stackrel{(b)}{=} I(\{\mathbf{A}_{k,\ell}\}_{k \in [m], \ell \in [p]}; f_{\mathbf{A}}(\alpha_i), i \in \mathcal{T}) \stackrel{(c)}{=} 0, \end{aligned} \quad (60)$$

where (a) is because the queries $\mathcal{Q}_{\mathcal{T}}^{(\theta)}$ and the data matrices $\mathbf{B}^{([V])}$ are generated independently of the encoded matrix $\tilde{\mathbf{A}}_{\mathcal{T}}$ and the matrix \mathbf{A} by (22)–(25), and the responses $\mathbf{Y}_{\mathcal{T}}^{(\theta)}$ (30) are the deterministic function of $\tilde{\mathbf{A}}_{\mathcal{T}}, \mathcal{Q}_{\mathcal{T}}^{(\theta)}$ and $\mathbf{B}^{([V])}$ by (25) and (26), such that $0 = I(\tilde{\mathbf{A}}_{\mathcal{T}}, \mathbf{A}; \mathcal{Q}_{\mathcal{T}}^{(\theta)}, \mathbf{B}^{([V])}) \geq I(\mathbf{A}; \mathcal{Q}_{\mathcal{T}}^{(\theta)}, \mathbf{B}^{([V])} | \tilde{\mathbf{A}}_{\mathcal{T}}) \geq 0$ and $I(\mathbf{A}; \mathbf{Y}_{\mathcal{T}}^{(\theta)} | \tilde{\mathbf{A}}_{\mathcal{T}}, \mathcal{Q}_{\mathcal{T}}^{(\theta)}, \mathbf{B}^{([V])}) = 0$; (b) follows by (17) and (24); (c) follows from (22), (9) and Lemma 1.

The security of our PSMM strategy based on polynomial codes follows from (2).

Privacy for PSMM Based on Polynomial Codes: By (23) and (25), the query elements $q_{\ell,j}^{(v)}(\alpha_{i_1}), \dots, q_{\ell,j}^{(v)}(\alpha_{i_T})$ sent to the workers \mathcal{T} are protected by T random noises $z_{\ell,j,1}^{(v)}, \dots, z_{\ell,j,T}^{(v)}$ chosen independently and uniformly from \mathbb{F}_q , for any $\ell \in [p], j \in [n]$ and $v \in [V]$, as shown below.

$$\begin{bmatrix} q_{\ell,j}^{(v)}(\alpha_{i_1}) \\ q_{\ell,j}^{(v)}(\alpha_{i_2}) \\ \vdots \\ q_{\ell,j}^{(v)}(\alpha_{i_T}) \end{bmatrix} = \underbrace{\begin{bmatrix} h_{\ell,j}^{(v)}(\alpha_{i_1}) \\ h_{\ell,j}^{(v)}(\alpha_{i_2}) \\ \vdots \\ h_{\ell,j}^{(v)}(\alpha_{i_T}) \end{bmatrix}}_{=\mathbf{h}_{\ell,j}^{(v)}} + \underbrace{\begin{bmatrix} \alpha_{i_1}^{d_1} & \alpha_{i_1}^{d_2} & \dots & \alpha_{i_1}^{d_T} \\ \alpha_{i_2}^{d_1} & \alpha_{i_2}^{d_2} & \dots & \alpha_{i_2}^{d_T} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{i_T}^{d_1} & \alpha_{i_T}^{d_2} & \dots & \alpha_{i_T}^{d_T} \end{bmatrix}}_{=\mathbf{F}_{\mathcal{T}}} \underbrace{\begin{bmatrix} z_{\ell,j,1}^{(v)} \\ z_{\ell,j,2}^{(v)} \\ \vdots \\ z_{\ell,j,T}^{(v)} \end{bmatrix}}_{=\mathbf{z}_{\ell,j}^{(v)}},$$

where

$$h_{\ell,j}^{(v)}(x) = \begin{cases} x^{b_{\ell,j}}, & \text{if } v = \theta \\ 0, & \text{if } v \neq \theta \end{cases}. \quad (61)$$

Recall from (9) that $\mathbf{F}_{\mathcal{T}}$ is invertible, whose inverse matrix is denoted by $(\mathbf{F}_{\mathcal{T}})^{-1}$. Then,

$$I(\theta; \mathcal{Q}_{\mathcal{T}}^{(\theta)}) \stackrel{(a)}{=} I(\theta; \{q_{\ell,j}^{(v)}(\alpha_i) : i \in \mathcal{T}\}_{\ell \in [p], j \in [n], v \in [V]}) \quad (62)$$

$$= I(\theta; \{\mathbf{h}_{\ell,j}^{(v)} + \mathbf{F}_{\mathcal{T}} \cdot \mathbf{z}_{\ell,j}^{(v)}\}_{\ell \in [p], j \in [n], v \in [V]}) \quad (63)$$

$$= I(\theta; \{(\mathbf{F}_{\mathcal{T}})^{-1} \cdot \mathbf{h}_{\ell,j}^{(v)} + \mathbf{z}_{\ell,j}^{(v)}\}_{\ell \in [p], j \in [n], v \in [V]}) \quad (64)$$

$$= H(\{(\mathbf{F}_{\mathcal{T}})^{-1} \cdot \mathbf{h}_{\ell,j}^{(v)} + \mathbf{z}_{\ell,j}^{(v)}\}_{\ell \in [p], j \in [n], v \in [V]}) \quad (65)$$

$$- H(\{(\mathbf{F}_{\mathcal{T}})^{-1} \cdot \mathbf{h}_{\ell,j}^{(v)} + \mathbf{z}_{\ell,j}^{(v)}\}_{\ell \in [p], j \in [n], v \in [V]} | \theta) \quad (66)$$

$$\stackrel{(b)}{=} H(\{(\mathbf{F}_{\mathcal{T}})^{-1} \cdot \mathbf{h}_{\ell,j}^{(v)} + \mathbf{z}_{\ell,j}^{(v)}\}_{\ell \in [p], j \in [n], v \in [V]})$$

$$- H(\{\mathbf{z}_{\ell,j}^{(v)}\}_{\ell \in [p], j \in [n], v \in [V]}) \quad (67)$$

$$\stackrel{(c)}{=} 0, \quad (68)$$

where (a) follows by (25); (b) holds because $(\mathbf{F}_{\mathcal{T}})^{-1} \cdot \mathbf{h}_{\ell,j}^{(v)}$ are constant numbers by (61) when θ is given, and $\mathbf{z}_{\ell,j}^{(v)}$ are generated independently of θ , for all $\ell \in [p], j \in [n], v \in [V]$, thus $H(\{(\mathbf{F}_{\mathcal{T}})^{-1} \cdot \mathbf{h}_{\ell,j}^{(v)} + \mathbf{z}_{\ell,j}^{(v)}\}_{\ell \in [p], j \in [n], v \in [V]} | \theta) = H(\{\mathbf{z}_{\ell,j}^{(v)}\}_{\ell \in [p], j \in [n], v \in [V]} | \theta) = H(\{\mathbf{z}_{\ell,j}^{(v)}\}_{\ell \in [p], j \in [n], v \in [V]})$; (c) is due to the fact that all the noises in $\{\mathbf{z}_{\ell,j}^{(v)}\}_{\ell \in [p], j \in [n], v \in [V]}$ are i.i.d. uniformly distributed on \mathbb{F}_q , and are generated independently of $\{(\mathbf{F}_{\mathcal{T}})^{-1} \cdot \mathbf{h}_{\ell,j}^{(v)}\}_{\ell \in [p], j \in [n], v \in [V]}$, such that $\{(\mathbf{F}_{\mathcal{T}})^{-1} \cdot \mathbf{h}_{\ell,j}^{(v)} + \mathbf{z}_{\ell,j}^{(v)}\}_{\ell \in [p], j \in [n], v \in [V]}$ and $\{\mathbf{z}_{\ell,j}^{(v)}\}_{\ell \in [p], j \in [n], v \in [V]}$ are identically and uniformly distributed over \mathbb{F}_q^{TVpn} , i.e., $H(\{(\mathbf{F}_{\mathcal{T}})^{-1} \cdot \mathbf{h}_{\ell,j}^{(v)} + \mathbf{z}_{\ell,j}^{(v)}\}_{\ell \in [p], j \in [n], v \in [V]}) = H(\{\mathbf{z}_{\ell,j}^{(v)}\}_{\ell \in [p], j \in [n], v \in [V]}) = TVpn$.

Further, we have

$$I(\theta; \mathcal{Q}_{\mathcal{T}}^{(\theta)}, \tilde{\mathbf{A}}_{\mathcal{T}}, \mathbf{B}^{([V])}, \mathbf{Y}_{\mathcal{T}}^{(\theta)}) \quad (69)$$

$$= I(\theta; \mathcal{Q}_{\mathcal{T}}^{(\theta)}) + I(\theta; \tilde{\mathbf{A}}_{\mathcal{T}}, \mathbf{B}^{([V])} | \mathcal{Q}_{\mathcal{T}}^{(\theta)}) \\ + I(\theta; \mathbf{Y}_{\mathcal{T}}^{(\theta)} | \mathcal{Q}_{\mathcal{T}}^{(\theta)}, \tilde{\mathbf{A}}_{\mathcal{T}}, \mathbf{B}^{([V])}) \quad (70)$$

$$\stackrel{(a)}{=} I(\theta; \mathcal{Q}_{\mathcal{T}}^{(\theta)}) \quad (71)$$

$$\stackrel{(b)}{=} 0, \quad (72)$$

where (a) is similar to (60) and (b) follows by (68).

Thus, the privacy of our PSMM strategy based on polynomial codes follows by (1).

We next turn to prove the security and privacy of the PSMM strategy based on Lagrange codes. Before that, a useful lemma is provided.

Lemma 3 (Generalized Cauchy Matrix [52]). *Let $\alpha_1, \dots, \alpha_T$ and β_1, \dots, β_T be pairwise distinct elements from \mathbb{F}_q , and v_1, \dots, v_T be T nonzero elements from \mathbb{F}_q . Denote by $f_k(x)$ a polynomial of degree $T - 1$*

$$f_k(x) = \prod_{j \in [T] \setminus \{k\}} \frac{x - \beta_j}{\beta_k - \beta_j}, \quad \forall k \in [T].$$

Then the following generalized Cauchy matrix is invertible over \mathbb{F}_q .

$$\begin{bmatrix} v_1 f_1(\alpha_1) & v_2 f_2(\alpha_1) & \dots & v_T f_T(\alpha_1) \\ v_1 f_1(\alpha_2) & v_2 f_2(\alpha_2) & \dots & v_T f_T(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ v_1 f_1(\alpha_T) & v_2 f_2(\alpha_T) & \dots & v_T f_T(\alpha_T) \end{bmatrix}_{T \times T}.$$

Security for PSMM Based on Lagrange Codes: For any subset $\mathcal{T} = \{i_1, i_2, \dots, i_T\} \subseteq [N]$ of size T ,

$$I(\mathbf{A}; \tilde{\mathbf{A}}_{\mathcal{T}}) \stackrel{(a)}{=} I(\{\mathbf{A}_{k,\ell}\}_{k \in [m], \ell \in [p]}; f_{\mathbf{A}}(\alpha_i), i \in \mathcal{T}) \stackrel{(b)}{=} 0,$$

where (a) follows from (17) and (35); (b) follows by (31), (33) and Lemmas 1 and 3.

Similar to (60), it is straightforward to prove $I(\mathbf{A}; \mathcal{Q}_{\mathcal{T}}^{(\theta)}, \tilde{\mathbf{A}}_{\mathcal{T}}, \mathbf{B}^{([V])}, \mathbf{Y}_{\mathcal{T}}^{(\theta)}) = I(\mathbf{A}; \tilde{\mathbf{A}}_{\mathcal{T}}) = 0$. Thus, the security of our PSMM strategy based on Lagrange codes follows from (2).

Privacy for PSMM Based on Lagrange Codes: By (34) and (36), the query elements $q_r^{(v)}(\alpha_{i_1}), \dots, q_r^{(v)}(\alpha_{i_T})$ sent to the workers \mathcal{T} are protected by the T random noises $z_{r,R+1}^{(v)}, \dots, z_{r,R+T}^{(v)}$, for any $r \in [R], v \in [V]$, as follows.

$$\begin{aligned} [q_r^{(v)}(\alpha_{i_1}) \dots q_r^{(v)}(\alpha_{i_T})]^T &= [h_r^{(v)}(\alpha_{i_1}) \dots h_r^{(v)}(\alpha_{i_T})]^T \\ &+ \underbrace{\begin{bmatrix} v_1(\alpha_{i_1})f_1(\alpha_{i_1}) & \dots & v_T(\alpha_{i_1})f_T(\alpha_{i_1}) \\ \vdots & \ddots & \vdots \\ v_1(\alpha_{i_T})f_1(\alpha_{i_T}) & \dots & v_T(\alpha_{i_T})f_T(\alpha_{i_T}) \end{bmatrix}}_{=\mathbf{F}'_{\mathcal{T}}} \begin{bmatrix} z_{r,R+1}^{(v)} \\ \vdots \\ z_{r,R+T}^{(v)} \end{bmatrix}, \end{aligned}$$

where

$$h_r^{(v)}(x) = \begin{cases} \prod_{j \in [R+T] \setminus \{r\}} \frac{x - \beta_j}{\beta_r - \beta_j}, & \text{if } v = \theta \\ 0, & \text{if } v \neq \theta \end{cases},$$

and

$$\begin{aligned} v_k(x) &= \prod_{j \in [R]} \frac{x - \beta_j}{\beta_{R+k} - \beta_j}, \quad \forall k \in [T], \\ f_k(x) &= \prod_{j \in [R+1:R+T] \setminus \{R+k\}} \frac{x - \beta_j}{\beta_{R+k} - \beta_j}, \quad \forall k \in [T]. \end{aligned}$$

By Lemma 3 again, $\mathbf{F}'_{\mathcal{T}}$ is invertible for any subset \mathcal{T} . Thus, similar to (62)–(72), it is easy to prove $I(\theta; \mathcal{Q}_{\mathcal{T}}^{(\theta)}, \tilde{\mathbf{A}}_{\mathcal{T}}, \mathbf{B}^{([V])}, \mathbf{Y}_{\mathcal{T}}^{(\theta)}) = I(\theta; \mathcal{Q}_{\mathcal{T}}^{(\theta)}) = I(\theta; \{q_r^{(v)}(\alpha_i) : i \in \mathcal{T}\}_{r \in [R], v \in [V]}) = 0$ for the PSMM strategy based on Lagrange codes, i.e., our PSMM strategy based on Lagrange codes is private.

B. Proof of Privacy for FPMM

We next prove the privacy for our two FPMM strategies based on polynomial codes and Lagrange codes.

For any $\mathcal{T} = \{i_1, i_2, \dots, i_T\} \subseteq [N]$ of size $|\mathcal{T}| = T$, the FPMM strategy based on polynomial codes satisfies

$$\begin{aligned} &I(\theta_1, \theta_2; \mathcal{Q}_{\mathcal{T}}^{(\theta_1)}, \mathcal{Q}_{\mathcal{T}}^{(\theta_2)}, \mathbf{A}^{([U])}, \mathbf{B}^{([V])}, \mathbf{Y}_{\mathcal{T}}^{(\theta_1, \theta_2)}) \\ &= I(\theta_1, \theta_2; \mathcal{Q}_{\mathcal{T}}^{(\theta_1)}, \mathcal{Q}_{\mathcal{T}}^{(\theta_2)}) + I(\theta_1, \theta_2; \mathbf{A}^{([U])}, \mathbf{B}^{([V])} | \mathcal{Q}_{\mathcal{T}}^{(\theta_1)}, \mathcal{Q}_{\mathcal{T}}^{(\theta_2)}) \\ &\quad + I(\theta_1, \theta_2; \mathbf{Y}_{\mathcal{T}}^{(\theta_1, \theta_2)} | \mathcal{Q}_{\mathcal{T}}^{(\theta_1)}, \mathcal{Q}_{\mathcal{T}}^{(\theta_2)}, \mathbf{A}^{([U])}, \mathbf{B}^{([V])}) \end{aligned}$$

$$\begin{aligned} &\stackrel{(a)}{=} I(\theta_1, \theta_2; \mathcal{Q}_{\mathcal{T}}^{(\theta_1)}, \mathcal{Q}_{\mathcal{T}}^{(\theta_2)}) \\ &\stackrel{(b)}{=} I(\theta_1, \theta_2; \{\rho_{k,\ell}^{(u)}(\alpha_i), q_{\ell,j}^{(v)}(\alpha_i) : i \in \mathcal{T}\}_{k \in [m], \ell \in [p], j \in [n], u \in [U], v \in [V]}) \\ &\stackrel{(c)}{=} 0, \end{aligned}$$

where (a) follows by the similar argument to (60); (b) is due to (44) and (45); (c) holds because the query elements $\{\rho_{k,\ell}^{(u)}(\alpha_i) : i \in \mathcal{T}\}$ and $\{q_{\ell,j}^{(v)}(\alpha_i) : i \in \mathcal{T}\}$ sent to workers \mathcal{T} are protected by random noises $\{\tilde{z}_{k,\ell,t}^{(u)}\}_{t \in [T]}$ and $\{z_{\ell,j,t}^{(v)}\}_{t \in [T]}$ by (42) and (43) respectively, for all $k \in [m], \ell \in [p], j \in [n], u \in [U], v \in [V]$, thus $I(\theta_1, \theta_2; \{\rho_{k,\ell}^{(u)}(\alpha_i), q_{\ell,j}^{(v)}(\alpha_i) : i \in \mathcal{T}\}_{k \in [m], \ell \in [p], j \in [n], u \in [U], v \in [V]}) = 0$ follows similar to (62)–(68).

Similarly, by (54)–(57) and Lemma 3, it is easy to prove that, the FPMM strategy based on Lagrange codes satisfies $I(\theta_1, \theta_2; \mathcal{Q}_{\mathcal{T}}^{(\theta_1)}, \mathcal{Q}_{\mathcal{T}}^{(\theta_2)}, \mathbf{A}^{([U])}, \mathbf{B}^{([V])}, \mathbf{Y}_{\mathcal{T}}^{(\theta_1, \theta_2)}) = I(\theta_1, \theta_2; \mathcal{Q}_{\mathcal{T}}^{(\theta_1)}, \mathcal{Q}_{\mathcal{T}}^{(\theta_2)}) = I(\theta_1, \theta_2; \{\rho_r^{(u)}(\alpha_i), q_r^{(v)}(\alpha_i) : i \in \mathcal{T}\}_{r \in [R], u \in [U], v \in [V]}) = 0$.

So the privacy of our two FPMM strategies follows by (4).

REFERENCES

- [1] J. Dean and L. A. Barroso, “The tail at scale,” *Communications of the ACM*, vol. 56, no. 2, pp. 74–80, 2013.
- [2] N. J. Yadwadkar, B. Hariharan, J. E. Gonzalez, and R. Katz, “Multi-task learning for straggler avoiding predictive job scheduling,” *The Journal of Machine Learning Research*, vol. 17, no. 1, pp. 3692–3728, 2016.
- [3] K.-H. Huang and J. A. Abraham, “Algorithm-based fault tolerance for matrix operations,” *IEEE Transactions on Computers*, vol. C-33, no. 6, pp. 518–528, 1984.
- [4] T. Herault and Y. Robert, *Fault-tolerance techniques for high-performance computing*. Springer, 2015.
- [5] S. Li and S. Avestimehr, “Coded computing: Mitigating fundamental bottlenecks in large-scale distributed computing and machine learning,” *Foundations and Trends in Communications and Information Theory*, vol. 17, no. 1, pp. 1–148, 2020.
- [6] K. Lee, C. Suh, and K. Ramchandran, “High-dimensional coded matrix multiplication,” in *2017 IEEE International Symposium on Information Theory (ISIT)*, pp. 2418–2422, IEEE, 2017.
- [7] M. Aliasgari, O. Simeone, and J. Kliewer, “Private and secure distributed matrix multiplication with flexible communication load,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2722–2734, 2020.
- [8] M. Kim and J. Lee, “Private secure coded computation,” *IEEE Communications Letters*, vol. 23, no. 11, pp. 1918–1921, 2019.
- [9] R. G. D’Oliveira, S. El Rouayheb, and D. Karpuk, “Gasp codes for secure distributed matrix multiplication,” *IEEE Transactions on Information Theory*, vol. 66, no. 7, pp. 4038–4050, 2020.
- [10] W.-T. Chang and R. Tandon, “On the capacity of secure distributed matrix multiplication,” in *2018 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, IEEE, 2018.
- [11] H. A. Nodehi, S. R. H. Najarkolaei, and M. A. Maddah-Ali, “Entangled polynomial coding in limited-sharing multi-party computation,” in *2018 IEEE Information Theory Workshop (ITW)*, pp. 1–5, IEEE, 2018.
- [12] J. Kakar, S. Ebadifar, and A. Sezgin, “On the capacity and straggler-robustness of distributed secure matrix multiplication,” *IEEE Access*, vol. 7, pp. 45783–45799, 2019.
- [13] J. Kakar, A. Khristoforov, S. Ebadifar, and A. Sezgin, “Uplink-downlink tradeoff in secure distributed matrix multiplication,” *arXiv preprint arXiv:1910.13849*, 2019.
- [14] N. Mital, C. Ling, and D. Gunduz, “Secure distributed matrix computation with discrete fourier transform,” *arXiv preprint arXiv:2007.03972*, 2020.
- [15] J. Zhu, Q. Yan, and X. Tang, “Improved constructions for secure multi-party batch matrix multiplication,” *IEEE Transactions on Communications*, vol. 69, pp. 7673–7690, 2021.
- [16] Q. Yu and A. S. Avestimehr, “Entangled polynomial codes for secure, private, and batch distributed matrix multiplication: Breaking the ‘cubic’ barrier,” in *2020 IEEE International Symposium on Information Theory (ISIT)*, pp. 245–250, IEEE, 2020.

- [17] J. Zhu and X. Tang, "Secure batch matrix multiplication from grouping lagrange encoding," *IEEE Communications Letters*, vol. 25, no. 4, pp. 1119–1123, 2020.
- [18] Q. Yu, M. A. Maddah-Ali, and A. S. Avestimehr, "Polynomial codes: an optimal design for high-dimensional coded matrix multiplication," in *Proceedings of the 31st International Conference on Neural Information Processing Systems*, pp. 4406–4416, 2017.
- [19] S. Dutta, M. Fahim, F. Haddadpour, H. Jeong, V. Cadambe, and P. Grover, "On the optimal recovery threshold of coded matrix multiplication," *IEEE Transactions on Information Theory*, vol. 66, no. 1, pp. 278–301, 2019.
- [20] Q. Yu, M. A. Maddah-Ali, and A. S. Avestimehr, "Straggler mitigation in distributed matrix multiplication: Fundamental limits and optimal coding," *IEEE Transactions on Information Theory*, vol. 66, no. 3, pp. 1920–1933, 2020.
- [21] S. Dutta, Z. Bai, H. Jeong, T. M. Low, and P. Grover, "A unified coded deep neural network training strategy based on generalized polydot codes for matrix multiplication," *arXiv preprint arXiv:1811.10751*, 2018.
- [22] Q. Yu, S. Li, N. Raviv, S. M. M. Kalan, M. Soltanolkotabi, and S. A. Avestimehr, "Lagrange coded computing: Optimal design for resiliency, security, and privacy," in *The 22nd International Conference on Artificial Intelligence and Statistics*, pp. 1215–1225, PMLR, 2019.
- [23] S. Li, M. A. Maddah-Ali, and A. S. Avestimehr, "Coded mapreduce," in *2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 964–971, IEEE, 2015.
- [24] S. Li, M. A. Maddah-Ali, Q. Yu, and A. S. Avestimehr, "A fundamental tradeoff between computation and communication in distributed computing," *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 109–128, 2017.
- [25] S. Li, Q. Yu, M. A. Maddah-Ali, and A. S. Avestimehr, "A scalable framework for wireless distributed computing," *IEEE/ACM Transactions on Networking*, vol. 25, no. 5, pp. 2643–2654, 2017.
- [26] K. Lee, M. Lam, R. Pedarsani, D. Papailiopoulos, and K. Ramchandran, "Speeding up distributed machine learning using codes," *IEEE Transactions on Information Theory*, vol. 64, no. 3, pp. 1514–1529, 2017.
- [27] S. Li, M. A. Maddah-Ali, and A. S. Avestimehr, "A unified coding framework for distributed computing with straggling servers," in *2016 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–6, IEEE, 2016.
- [28] S. Dutta, V. Cadambe, and P. Grover, "Short-dot: Computing large linear transforms distributedly using coded short dot products," *Advances In Neural Information Processing Systems*, vol. 29, 2016.
- [29] R. Tandon, Q. Lei, A. G. Dimakis, and N. Karampatziakis, "Gradient coding: Avoiding stragglers in distributed learning," in *International Conference on Machine Learning*, pp. 3368–3376, PMLR, 2017.
- [30] W.-T. Chang and R. Tandon, "On the upload versus download cost for secure and private matrix multiplication," in *2019 IEEE Information Theory Workshop (ITW)*, pp. 1–5, IEEE, 2019.
- [31] H. Sun and S. A. Jafar, "The capacity of private computation," *IEEE Transactions on Information Theory*, vol. 65, no. 6, pp. 3880–3897, 2018.
- [32] S. Li, M. Yu, C.-S. Yang, A. S. Avestimehr, S. Kannan, and P. Viswanath, "Polyshard: Coded sharding achieves linearly scaling efficiency and security simultaneously," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 249–261, 2020.
- [33] J. Zhu, Q. Yan, X. Tang, and S. Li, "Symmetric private polynomial computation from lagrange encoding," *IEEE Transactions on Information Theory*, vol. 68, no. 4, pp. 2704–2718, 2022.
- [34] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," in *Proceedings of IEEE 36th Annual Foundations of Computer Science*, pp. 41–50, IEEE, 1995.
- [35] N. B. Shah, K. Rashmi, and K. Ramchandran, "One extra bit of download ensures perfectly private information retrieval," in *2014 IEEE International Symposium on Information Theory*, pp. 856–860, IEEE, 2014.
- [36] H. Sun and S. A. Jafar, "The capacity of private information retrieval," *IEEE Transactions on Information Theory*, vol. 63, no. 7, pp. 4075–4088, 2017.
- [37] H. Sun and S. A. Jafar, "The capacity of robust private information retrieval with colluding databases," *IEEE Transactions on Information Theory*, vol. 64, no. 4, pp. 2361–2370, 2017.
- [38] K. Banawan and S. Ulukus, "The capacity of private information retrieval from coded databases," *IEEE Transactions on Information Theory*, vol. 64, no. 3, pp. 1945–1956, 2018.
- [39] J. Zhu, Q. Yan, C. Qi, and X. Tang, "A new capacity-achieving private information retrieval scheme with (almost) optimal file length for coded servers," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1248–1260, 2019.
- [40] J. Zhu, Q. Yan, X. Tang, and Y. Miao, "Capacity-achieving private information retrieval schemes from uncoded storage constrained servers with low sub-packetization," *IEEE Transactions on Information Theory*, vol. 67, no. 8, pp. 5370–5386, 2021.
- [41] M. Kim, H. Yang, and J. Lee, "Private coded matrix multiplication," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1434–1443, 2019.
- [42] Z. Jia and S. A. Jafar, "X-secure t-private information retrieval from mds coded storage with byzantine and unresponsive servers," *IEEE Transactions on Information Theory*, vol. 66, no. 12, pp. 7427–7438, 2020.
- [43] Z. Jia, H. Sun, and S. A. Jafar, "Cross subspace alignment and the asymptotic capacity of x-secure t-private information retrieval," *IEEE Transactions on Information Theory*, vol. 65, no. 9, pp. 5783–5798, 2019.
- [44] J. Li and C. Hollanti, "Private and secure distributed matrix multiplication schemes for replicated or mds-coded servers," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 659–669, 2022.
- [45] A. V. Smirnov, "The bilinear complexity and practical algorithms for matrix multiplication," *Computational Mathematics and Mathematical Physics*, vol. 53, no. 12, pp. 1781–1795, 2013.
- [46] V. Strassen, "Gaussian elimination is not optimal," *Numerische mathematik*, vol. 13, no. 4, pp. 354–356, 1969.
- [47] K. Vaidya and B. S. Rajan, "Distributed computation: Privacy, straggler mitigation, and security against colluding workers," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*, pp. 1–6, IEEE, 2020.
- [48] M. Kim, H. Yang, and J. Lee, "Fully private coded matrix multiplication from colluding workers," *IEEE Communications Letters*, vol. 25, no. 3, pp. 730–733, 2020.
- [49] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
- [50] A. Sedoglavic, *Fast matrix multiplication algorithms*. Accessed: Dec. 2021. [Online]. Available: <https://fmm.univ-lille.fr/>.
- [51] J. Von Zur Gathen and J. Gerhard, *Modern computer algebra*. Cambridge university press, 2013.
- [52] S. Lin and D. J. Costello, *Error Control Coding: Fundamentals and Applications*. Prentice-Hall, 1983.