Differentially Private Secure Multiplication with Erasures and Adversaries

Haoyang Hu, Viveck R. Cadambe

Abstract

We consider a private distributed multiplication problem involving N computation nodes and T colluding nodes. Shamir's secret sharing algorithm provides perfect information-theoretic privacy, while requiring an honest majority, i.e., $\mathsf{N} \geq 2\mathsf{T}+1$. Previous work [1] investigates the honest minority setting but does not incorporate the error correction capabilities of Shamir's secret-sharing algorithm, as it does not employ a polynomial-based structure. This paper explores a polynomial-based coding scheme that ensures the differential privacy (DP) of the input data. We characterize the achievable privacy-utility tradeoff, where privacy is quantified by the DP parameter and utility by the mean square error, showing that the tradeoff can approach the converse bound as closely as desired. The proposed scheme inherits the capability of the Reed-Solomon (RS) code to resist erasures and adversaries. We utilize a modified Berlekamp–Welch algorithm over the real number field to detect adversarial nodes. The effectiveness of the coding scheme is verified via both theoretical analysis and simulations.

I. Introduction

Secure multi-party computation allows multiple parties to collaboratively perform a computation over their private inputs while preserving the confidentiality of those inputs[2]. A significant contribution to this area is Shamir's secret sharing [3], a method rooted in RS codes [4], providing a framework for ensuring information-theoretic privacy. Consider an N-node secure computation system designed to compute the product of two random variables $A, B \in \mathbb{F}$, where $\mathbb{F}$ is a finite field. Let $\{R_t, S_t\}_{t=1}^{\mathsf{T}}$ be independent random noises uniformly distributed over the field, Shamir's secret sharing algorithm encodes A, B by constructing polynomials,

$$p_1(x) = A + \sum_{t=1}^{\mathsf{T}} R_t x^t, p_2(x) = B + \sum_{t=1}^{\mathsf{T}} S_t x^t \tag{1}$$

Node i receives $p_1(x_i)$ and $p_2(x_i)$, where $\{x_1, \cdots, x_{\mathsf{N}}\}$ denote non-zero distinct elements over the field $\mathbb{F}$. Any set of T colluding nodes fail to recover A and B, but at least $2T+1$ nodes are required to obtain the product AB by interpolating the $2\mathsf{T}$-degree polynomial $p_1(x)p_2(x)$. In other words, perfect information-theoretic privacy requires an honest majority to ensure security and correctness. Because of the error-correction properties of RS codes, secure computation schemes based on Shamir's secret sharing can tolerate node erasures and adversarial nodes that report erroneous values, so long as the number of erasures and adversarial nodes are bounded by certain thresholds.

Haoyang Hu and Viveck R. Cadambe are with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, 30332 USA. (E-mail: {haoyang.hu, viveck}@gatech.edu)

In several practical applications, especially in machine learning[5], a controlled amount of privacy leakage is acceptable, rather than enforcing perfect information-theoretic privacy[5]. Differential Privacy (DP) offers a standard framework for quantifying and managing this leakage [6]. Recent work [1] has explored secure multiplication over the real field and within the honest minority setting, i.e., $\mathsf{T} < \mathsf{N} < 2\mathsf{T}+1$, and established a tight privacy-accuracy tradeoff through a DP perspective. Technically, [1] introduces multiple layers of noise to the inputs, aiming to achieve DP under T-node collusion while improving the accuracy of estimates. However, the design in [1] is divorced from the polynomial structure of RS codes and Shamir secret sharing. Notably, the scheme of [1] is asymmetric, requiring one node to implement a unique noise structure distinct from the others. This dependency creates a critical vulnerability, as, unlike RS codes, successful decoding cannot be assured if the designated node either fails (acting as an erasure) or if a subset of nodes behaves maliciously (acting as adversaries). This prompts the exploration of whether a polynomial-based coding scheme can be developed for the honest minority setting. Such a scheme would aim to provide input data privacy while preserving the inherent robustness of RS codes in tolerating both erasures and adversarial actions. This is the main contribution of this paper.

We develop a novel polynomial-based coding scheme over the real field for differentially private secure multiplication in the presence of erasures and adversaries. We characterize the achievable privacy-accuracy tradeoff of our scheme, with privacy quantified by the DP parameter and accuracy quantified by the mean square error. Our scheme achieves performance comparable to that of [1], while offering resilience against erasers and adversaries. Specifically, our analysis shows that our achievable privacy-accuracy trade-off approaches the converse bound of [1], obtained in the absence of erasures and adversaries, arbitrarily closely. We operate within the real domain and enables the use of a modified version of the Berlekamp–Welch algorithm [7] to detect and correct adversaries. We verify the correctness of the algorithm via both theoretical analysis and numerical simulations.

Related works: Coding techniques are widely employed in distributed systems not only to improve resilience against stragglers by introducing structured redundancy [8], [9], [10], [11], [12] but also to ensure the privacy of sensitive inputs [13], [14], [15], [16], [17], [18], [19], [20]. These works extend the standard Shamir's secret-sharing algorithm by introducing additional constraints on the distributed systems, and develop novel coding schemes that ensure both exact computation and perfect information-theoretic privacy. However, accuracy loss is inevitable by quantization when converting from the real domain to a finite domain. To mitigate the negative effects, [1], [21], [22], [23], [24] explore coded computing techniques over the real domain, where enforcing strict information-theoretic privacy is not feasible. Specifically, [23], [24] explore the use of DP to evaluate the privacy-utility tradeoff in coded computing settings like this work. While these works focus on (ϵ, δ)-DP with $\delta > 0$, our work specifically considers ϵ-DP. In addition, error correction codes over the real field are explored in [25], [26], where the threshold of errors is specified. This paper does not impose such constraints; instead, we exploit the unique properties of the proposed schemes to detect and locate errors.

Notations: Calligraphic symbols denote sets, bold symbols denote matrices and vectors, and sans-serif symbols denote system parameters. Let $\mathbf{1}$ denote an all-ones column vector. For a positive integer a, we let $[a] \triangleq \{1, \dots, a\}$. For a matrix $\mathbf{A}$, let $\mathbf{A}^T$ denote its transpose. For functions f and g and for all large enough values of x, we write $f(x) = O(g(x))$ if there exists a positive real number M and a real number $a_0 \in \mathbb{R}$ such that $|f(x)| \leq M|g(x)|$

for all $x \geq a_0$.

II. System Model and Main Results

In this section, we introduce the considered system model and then present the main results of this paper.

A. System Model

We consider a distributed computing system in which N nodes collaboratively perform the multiplication of two input random variables $A, B \in \mathbb{R}$. These random variables are assumed to be statistically independent and satisfy the constraints that $\mathbb{E}[A^2], \mathbb{E}[B^2] \leq \eta$ with $\eta \geq 0$.

Let each node $i \in [\mathsf{N}]$ store the noisy version of input A and B in this setting, where

$$\tilde{A}_i = A + \tilde{R}_i, \quad \tilde{B}_i = B + \tilde{S}_i, \tag{2}$$

where $\{\tilde{R}_i, \tilde{S}_i\}_{i=1}^{\mathsf{N}}$ are random variables that are independent with A, B. We assume random noises $\{\tilde{R}_i, \tilde{S}_i\}_{i=1}^{\mathsf{N}}$ have zero means. Node $i \in [\mathsf{N}]$ then outputs

$$\tilde{C}_i = \tilde{A}_i \tilde{B}_i. \tag{3}$$

After the local computation, a decoder collects $\{Y_i\}_{i=1}^{\mathsf{N}}$, and $Y_i \in \mathbb{R} \cup \{\varepsilon\}$ where ε represents the message is erased. We assume that the number of erasures is at most E, and that at most A nodes are malicious adversaries whose output can be inconsistent with the computation. Let $\mathcal{E}$ denote the indices of erasures, i.e., $\mathcal{E} = \{i | Y_i = \varepsilon\}$, and $\mathcal{A}$ denote the indices of errors, i.e., $\mathcal{A} = \{i | Y_i \neq \tilde{C}_i\}$. Specifically, let $\varepsilon_i = Y_i - \tilde{C}_i$ represent the added error value at node $i \in \mathcal{A}$. The decoder then applies a decoding function $d : (\mathbb{R} \cup \{\varepsilon\})^{\mathsf{N}} \to \mathbb{R}$ to estimate the desired multiplication result, i.e.,

$$\tilde{C} = d(Y_1, Y_2, \cdots, Y_{\mathsf{N}}). \tag{4}$$

Here we define T-node ϵ-DP to mean that the data of any T nodes satisfies ϵ-DP with respect to the original input data.

Definition 1 (T-node ϵ-DP): A coding scheme $\mathcal{C}$ with random noise variables $\{\tilde{R}_i, \tilde{S}_i\}_{i=1}^{N}$ satisfies T-node ϵ-DP for $\epsilon > 0$ if for any $A_0, B_0, A_1, B_1 \in \mathbb{R}$ satisfying $\|A_0 - A_1\|_\infty \leq 1$, $\|B_0 - B_1\|_\infty \leq 1$, the following requirement holds for all subsets $\mathcal{T} \subseteq [\mathsf{N}]$ with $|\mathcal{T}| = \mathsf{T}$, and for all subsets $\mathcal{B} \subset \mathbb{R}^{1\times\mathsf{T}}$ in the Borel σ-field,

$$\max\left(\frac{\mathbb{P}\left(\mathbf{Y}_{\mathcal{T}}^{(0)} \in \mathcal{B}\right)}{\mathbb{P}\left(\mathbf{Y}_{\mathcal{T}}^{(1)} \in \mathcal{B}\right)}, \frac{\mathbb{P}\left(\mathbf{Z}_{\mathcal{T}}^{(0)} \in \mathcal{B}\right)}{\mathbb{P}\left(\mathbf{Z}_{\mathcal{T}}^{(1)} \in \mathcal{B}\right)}\right) \leq e^{\epsilon}, \tag{5}$$

where $\mathbf{Y}_{\mathcal{T}}^{(\ell)} \triangleq \begin{bmatrix} A_\ell + \tilde{R}_{t_1} & A_\ell + \tilde{R}_{t_2} & \cdots & A_\ell + \tilde{R}_{t_{\mathsf{T}}} \end{bmatrix}$ and $\mathbf{Z}_{\mathcal{T}}^{(\ell)} \triangleq \begin{bmatrix} B_\ell + \tilde{S}_{t_1} & B_\ell + \tilde{S}_{t_2} & \cdots & B_\ell + \tilde{S}_{t_{\mathsf{T}}} \end{bmatrix}$ with $\ell \in \{0, 1\}$, $\mathcal{T} = \{t_1, t_2, \cdots, t_{\mathsf{T}}\}$.

A secure multiplication coding scheme $\mathcal{C}(\eta, \epsilon, \mathsf{T}, \mathsf{A}, \mathsf{E})$ specifies a joint distribution of $\{\tilde{R}_i, \tilde{S}_i\}_{i=1}^{\mathsf{N}}$ that satisfies T-node ϵ-DP and a decoding function d with output $\tilde{C}$ based on knowledge of E and A. For a given coding scheme, define $\mathtt{MSE}(\mathcal{C})$ as the maximum mean squared error over all possible erasure and adversary patterns.

Definition 2 (Mean square error): For a coding scheme $\mathcal{C}$ consisting of the joint distribution of $\{\tilde{R}_i, \tilde{S}_i\}_{i=1}^{\mathsf{N}}$ and the decoding function d, the mean square error $(\mathtt{MSE})$ is defined as $\mathtt{MSE}(\mathcal{C}) = \sup_{\mathbf{Y}\subseteq(\mathbb{R}\cup\{\varepsilon\})^{\mathsf{N}}} \mathbb{E}[|d(\mathbf{Y}) - AB|^2]$, with $\mathbf{Y}$ satisfying $|\{i|Y_i = \varepsilon\}| \leq \mathsf{E}$, and $|\{i|Y_i \neq \tilde{C}_i\}| \leq \mathsf{A}$.

B. Main Results

Definition 3: Define $(\sigma^*(\epsilon))^2$ as the smallest noise variance among all noisy mechanisms achieving single user ϵ-DP. For $\epsilon > 0$, let $\mathcal{S}_\epsilon(\mathbb{P})$ denote the set of all real-valued random variables that satisfy ϵ-DP, i.e., $X \in \mathcal{S}_\epsilon(\mathbb{P})$ if and only if,

$$\sup_{X',X'',\mathcal{B}\in\mathbb{R},|X'-X''|\leq 1} \frac{\mathbb{P}(X'+X\in\mathcal{B})}{\mathbb{P}(X''+X\in\mathcal{B})} \leq e^\epsilon. \tag{6}$$

Let $L^2(\mathbb{P})$ denote the set of all real-values random variables with finite variance. Hence

$$(\sigma^*(\epsilon))^2 = \inf_{X\in\mathcal{S}_\epsilon(\mathbb{P})\cap L^2(\mathbb{P})} \mathbb{E}\left[(X - \mathbb{E}[X])^2\right]. \tag{7}$$

The function $(\sigma^*(\epsilon))^2$ is characterized in [27] as follows.

$$(\sigma^*(\epsilon))^2 = \frac{2^{2/3}e^{-2\epsilon/3}(1+e^{-2\epsilon/3}) + e^{-\epsilon}}{(1-e^{-\epsilon})^2}. \tag{8}$$

Our main result is the following theorem, which presents an achievable trade-off between the mean square error $\mathtt{MSE}(\mathcal{C})$ and the differential privacy parameter ϵ under the proposed coding scheme $\mathcal{C}$.

Theorem 1: For a positive integer N and non-negative integers $\mathsf{T}, \mathsf{E}, \mathsf{A}$ such that $\mathsf{N} \geq \mathsf{T} + \mathsf{E} + 2\mathsf{A} + 1$, there exists a secure multiplication scheme $\mathcal{C}$ that guarantees T-node ϵ-DP in presence of at most E erasures and at most A adversaries with the mean square error $\mathtt{MSE}(\mathcal{C})$ satisfying, for any $\delta > 0$,

$$\mathtt{MSE}(\mathcal{C}) \leq \frac{\eta^2}{(1+\mathtt{SNR}^*)^2} + \delta, \tag{9}$$

where $\mathtt{SNR}^* = \frac{\eta}{(\sigma^*(\epsilon))^2}$.

See Section III-B and III-C for the proof.

Remark 1: For the case where $\mathsf{N} \geq 2\mathsf{T} + \mathsf{E} + 2\mathsf{A} + 1$,$\mathtt{MSE}(\mathcal{C})$ can be achieved by applying real-valued Shamir's secret sharing [21] for every $\epsilon > 0$. The result for the special case where $\mathsf{E} = \mathsf{A} = 0$ is established in [1]. The primary contribution of this paper addresses the general case where $\mathsf{E} \neq 0$ and $\mathsf{A} \neq 0$.

Remark 2: Previous work [1] has established the lower bound $\mathtt{MSE}$ for all additive noise privacy mechanisms that satisfy T-node ϵ-DP with linear decoders, as stated in Corollary 2.3.1, and has proven the tightness of this bound for its scheme. A linear decoder, in this context, processes all outputs by replacing a subset of the coordinates affected by erasures or adversaries, then applies a linear operation to the remaining outputs. The coefficients of this linear operation depend solely on the remaining nodes. Our work achieves the same privacy-utility tradeoff as [1] under the constraints of additive noises and linear decoders, and thus, the optimality of our approach is automatically implied by the results in [1].

III. Proposed Coding Schemes

In this section, we introduce a N-node secure multiplication coding scheme that achieves T-node ϵ-DP in the presence of at most E erased nodes and at most A adversary nodes in Section III-A. Here $\mathsf{T}, \mathsf{E}, \mathsf{A}$ are non-negative integers satisfying $\mathsf{N} \geq \mathsf{T} + \mathsf{E} + 2\mathsf{A} + 1$. Section III-B verifies the T-node ϵ-DP property. Upon receiving results from $\mathsf{N} - \mathsf{E}$ nodes, the decoder can correct up to A errors using the techniques outlined in Section III-D, resulting in $\mathsf{N} - \mathsf{E} - 2\mathsf{A}$ accurate computation outputs. Given the condition $\mathsf{N} \geq \mathsf{T} + \mathsf{E} + 2\mathsf{A} + 1$, the decoder is guaranteed to obtain at least $\mathsf{T} + 1$ accurate computation results. In Section III-C, we then analyze the accuracy for estimating the product based on these $\mathsf{T} + 1$ reliable messages.

A. Coding Schemes

Let $\{R_t, S_t\}_{t=1}^{\mathsf{T}}$ be statistically independent random variables with zero mean, and the choice of the distribution $\{R_t, S_t\}_{t=1}^{\mathsf{T}}$ will be specified in Section III-B to guarantee T-node ϵ-DP for a fixed ϵ.

We will then present a sequence of coding schemes indexed by positive integers n, that achieve the privacy-utility tradeoff described in Theorem 1 as $n \to \infty$. For the coding scheme with $\mathsf{T} > 1$ [1], let

$$p_A(x) = (A + R_1) + \frac{1}{n} \sum_{t=1}^{\mathsf{T}-1} R_{t+1} x^t + \frac{1}{n^{3/2}} R_1 x^{\mathsf{T}}, \tag{10a}$$

$$p_B(x) = (B + S_1) + \frac{1}{n} \sum_{t=1}^{\mathsf{T}-1} S_{t+1} x^t + \frac{1}{n^{3/2}} S_1 x^{\mathsf{T}}. \tag{10b}$$

Select N distinct non-zero real numbers $\{x_i\}_{i=1}^{\mathsf{N}}$, and each node $i \in [\mathsf{N}]$ obtains the encoded data as $\tilde{A}_i = p_A(x_i), \tilde{B}_i = p_B(x_i)$. The coding scheme can be viewed as a $(\mathsf{N}, \mathsf{T}+1)$ real-valued RS code with messages $\{A + R_1, \frac{1}{n} R_2, \cdots, \frac{1}{n} R_{\mathsf{T}}, \frac{1}{n^{3/2}} R_1\}$.

For the case with $\mathsf{T} = 1$, the received coded data of node $i \in \mathsf{N}$ can be represented as

$$p_A(x_i) = (A + R_1) + \frac{1}{n^{3/2}} R_1 x_i, \quad p_B(x_i) = (B + S_1) + \frac{1}{n^{3/2}} S_1 x_i. \tag{11}$$

Remark 3: [1] proposed a coding scheme with $\mathsf{N} = \mathsf{T} + 1$. The first T nodes apply three layers of noise with different magnitudes, while the last node applies only the first layer of noise. However, this design is highly vulnerable, as the system fails to estimate the desired product if the last node is either erased or acts maliciously.

The intuition for the coding scheme design is as follows. The noise added to the input A can be interpreted as a superposition of three layers, distinguished by their magnitudes[2]: R_1 with magnitude $O(1)$, $\{\frac{1}{n} R_{t+1} x^t\}_{t=1}^{\mathsf{T}-1}$ with magnitude $O\left(\frac{1}{n}\right)$ and $\frac{1}{n^{3/2}} R_1 x^{\mathsf{T}}$ with magnitude $O\left(\frac{1}{n^{3/2}}\right)$. The first layer, R_1, is carefully designed with an appropriate distribution and variance to ensure a DP parameter ϵ. The third layer of noise, with magnitude $O\left(\frac{1}{n^{3/2}}\right)$ and correlated to the first layer is to mitigate the negative impact of R_1 on accuracy. The second layer of noise of magnitude $O\left(\frac{1}{n}\right)$ prevents an adversary that controls up to T nodes from accessing the third layer. This is achieved by letting $\lim_{n\to\infty} \frac{1}{n^{3/2}} / \frac{1}{n} = 0$, effectively hiding the third layer. Simultaneously, $\mathsf{T} + 1$ nodes can remove the second layer to improve estimation accuracy.

[1] The terms $\frac{1}{n}$ and $\frac{1}{n^{3/2}}$ in (10) can be replaced by other functions of n as long as the constrains in (7) of [1] are satisfied.

[2] Here we consider the setting with $\mathsf{T} > 1$. For the case $\mathsf{T} = 1$, only the first and the last layers of noise, i.e., R_1 and $\frac{1}{n^{3/2}} x_i R_1$, remain.

B. *Differential Privacy Analysis*

Due to the symmetry of the proposed coding scheme, it suffices to demonstrate that the input A satisfies T-node ϵ-DP and describe the design of additive noise $\{R_t\}_{t=1}^{\mathsf{T}}$. The DP analysis for the input B and the selection of $\{S_t\}_{t=1}^{\mathsf{T}}$ can be derived in a similar manner. To facilitate later analysis, we rewrite (10) based on the magnitude of each term as follows.

$$\tilde{A}_i = (A+R_1) + \frac{1}{n}\begin{bmatrix} R_2 & \cdots & R_{\mathsf{T}} \end{bmatrix} \mathbf{g}_i + \frac{1}{n^{3/2}} h_i R_1, \tag{12}$$

where $\mathbf{g}_i = \begin{bmatrix} x_i & x_i^2 & \cdots & x_i^{\mathsf{T}-1} \end{bmatrix}^T$ and $h_i = x_i^{\mathsf{T}}$. Let $\mathbf{G} = \begin{bmatrix} \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_{\mathsf{N}} \end{bmatrix}^T$, $\mathbf{h} = \begin{bmatrix} h_1 & h_2 & \cdots & h_{\mathsf{N}} \end{bmatrix}^T$, and then let the Vandermonde matrix $\mathbf{M} = \begin{bmatrix} \mathbf{1} & \mathbf{G} & \mathbf{h} \end{bmatrix}$. Based on the property of Vandermonde matrix, every $(\mathsf{T}-1)\times(\mathsf{T}-1)$, $\mathsf{T}\times\mathsf{T}$ and $(\mathsf{T}+1)\times(\mathsf{T}+1)$ submatrix of $\mathbf{M}$ is guaranteed to be invertible.

We begin with the distributions of the independent noise variables $\{R_t\}_{t=1}^{\mathsf{T}}$. For a given DP parameter ϵ, let $\sigma^2 = (\sigma^*(\epsilon))^2 + \delta'$, where $\delta' > 0$ and $(\sigma^*(\epsilon))^2$ is defined as (8). For a fixed value σ, let ϵ^* be defined as,

$$\epsilon^* = \inf_{Z, \mathbb{E}[Z^2] \geq \sigma^2} \sup_{\mathcal{B}, A_0, A_1 \in \mathbb{R}, |A_0 - A_1| \leq 1} \ln\left(\frac{\mathbb{P}(A_0 + Z \in \mathcal{B})}{\mathbb{P}(A_1 + Z \in \mathcal{B})}\right), \tag{13}$$

where $Z \in \mathbb{R}$ and $\mathbb{E}[Z] = 0$. Note that the noise variance $\mathbb{E}[Z^2]$ is strictly larger than $(\sigma^*(\epsilon))^2$. As $\sigma^*(\epsilon)$ is a strictly decreasing function with the DP parameter ϵ (as evident from the expression of ϵ^* in (8)) and $\mathbb{E}[Z^2] > (\sigma^*(\epsilon))^2$, it follows that $\epsilon^* < \epsilon$. For a DP parameter $\bar{\epsilon}$ with $\epsilon^* < \bar{\epsilon} < \epsilon$, there exists a random noise Z^* such that $\mathbb{E}[(Z^*)^2] \leq \sigma^2$satisfying,

$$\sup_{\mathcal{B}\in\mathbb{R}, -1<\lambda<1} \frac{\mathbb{P}(A + Z^* \in \mathcal{B})}{\mathbb{P}(A + Z^* + \lambda \in \mathcal{B})} \leq e^{\bar{\epsilon}} \leq e^{\epsilon}. \tag{14}$$

Let the addictive noise R_1 follow the same distribution as Z^*, and it follows that $A+R_1$ guarantees ϵ-DP. The noise variables $R_2, R_3, \cdots, R_{\mathsf{T}}$ are chosen as independent unit-variance Laplace random variables, each independent of R_1.

For the case with $\mathsf{T} \geq 2$, we assume that the first T nodes collude, i.e., the colluding node set is $\mathcal{T} = \{1, 2\cdots, \mathsf{T}\}$. For any other colluding set of T nodes, the argument we outline below will follow similarly due to the inherent symmetry in our coding scheme. The colluding nodes receive: $\mathbf{Z} = (A+R_1)\mathbf{1} + \bar{\mathbf{G}}\begin{bmatrix} \frac{1}{n^{3/2}}R_1 & \frac{1}{n}R_2 & \cdots & \frac{1}{n}R_{\mathsf{T}} \end{bmatrix}^T$, where $\bar{\mathbf{G}} = \begin{bmatrix} h_1 & h_2 & \cdots & h_{\mathsf{T}} \\ \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_{\mathsf{T}} \end{bmatrix}^T$. We will now show that there is a full rank matrix $\mathbf{P}$ such that $\mathbf{Z}' = \mathbf{P}\mathbf{Z}$, where

$$\mathbf{Z}' = \begin{bmatrix} A + \left(1 + \frac{1}{n^{3/2}\mathbf{g'}_1^T\mathbf{1}}\right)R_1 & A + \frac{1 + n^{3/2}\mathbf{g'}_1^T\mathbf{1}}{n\mathbf{g'}_2^T\mathbf{1}}R_2 & \cdots & A + \frac{1 + n^{3/2}\mathbf{g'}_1^T\mathbf{1}}{n\mathbf{g'}_{\mathsf{T}}^T\mathbf{1}}R_{\mathsf{T}} \end{bmatrix}^T. \tag{15}$$

As the matrix $\bar{\mathbf{G}}$ has a full rank of T according to the designed scheme, colluders can, through a one-to-one map of $\mathbf{Z}$ obtain:

$$(A+R_1)\bar{\mathbf{G}}^{-1}\mathbf{1} + \begin{bmatrix} \frac{1}{n^{3/2}}R_1 & \frac{1}{n}R_2 & \cdots & \frac{1}{n}R_{\mathsf{T}} \end{bmatrix}^T.$$

Let $\mathbf{g'}_i^T$ with $i \in [\mathsf{T}]$ denote the i-th row of the matrix $\bar{\mathbf{G}}^{-1}$, and then $\mathbf{g'}_i^T\mathbf{1}$ represents the i-th element of the column vector $\bar{\mathbf{G}}^{-1}\mathbf{1}$. We now argue that $\mathbf{g'}_i^T\mathbf{1} \neq 0$. Due to the fact that $\bar{\mathbf{G}}^{-1}\bar{\mathbf{G}} = \mathbf{I}$, we have that $\mathbf{g'}_1^T\begin{bmatrix} h_1 & h_2 & \cdots & h_{\mathsf{T}} \end{bmatrix}^T = 1$ and $\mathbf{g'}_1^T\begin{bmatrix} \mathbf{g_1} & \mathbf{g_2} & \cdots & \mathbf{g}_{\mathsf{T}} \end{bmatrix}^T = \mathbf{0}^T$. The first equation shows that $\mathbf{g'}_1^T$ is not an all-zero row vector. According to the coding scheme, the matrix $\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_{\mathsf{T}} \end{bmatrix}^T$ is full-rank, together with $\mathbf{g}'^T_1 \begin{bmatrix} \mathbf{g_1} & \mathbf{g_2} & \cdots & \mathbf{g}_{\mathsf{T}} \end{bmatrix}^T = \mathbf{0}^T$, $\mathbf{g}'^T_i\mathbf{1}$ cannot be zero.

We can then normalize the first component of the mapped $\mathbf{Z}$ and obtain $A + \left(1 + \frac{1}{n^{3/2}\mathbf{g}'^T_1\mathbf{1}}\right) R_1$. Next, we can use $A + \left(1 + \frac{1}{n^{3/2}\mathbf{g}'^T_1\mathbf{1}}\right) R_1$ to remove R_1 terms [3] in the other component of $\mathbf{Z}$. Hence we can derive $\mathbf{Z}'$ shown in (15).

Let $\mathbf{Z}' = \begin{bmatrix} Z'_1 & Z'_2 & \cdots & Z'_{\mathsf{T}} \end{bmatrix}^T$, and each Z'_i with $i \in [\mathsf{T}]$ is expressed as a linear combination of A and R_i. According to the post-processing property of differential privacy [6] (performing arbitrary computations on the output of a DP mechanism does not increase the privacy loss), $\mathbf{Z}' = \mathbf{PZ}$ inherits the DP guarantee of $\mathbf{Z}$, i.e., $\mathbf{Z}'$ remains DP with at least the same level of privacy as $\mathbf{Z}$. To complete the proof, it therefore suffices to show that $\mathbf{Z}'$ is ϵ-DP.

For $2 \le i \le \mathsf{T}$, the i-th term of Z'_i is $A + \frac{1+n^{3/2}\mathbf{g}'^T_1\mathbf{1}}{n\mathbf{g}'^T_i\mathbf{1}} R_i$, where the second term represents a Laplace random variable with variance $\left(\frac{1+n^{3/2}\mathbf{g}'^T_1\mathbf{1}}{n\mathbf{g}'^T_i\mathbf{1}}\right)^2$. Since the added Laplace random noise with distribution Lap$(\frac{1}{\epsilon})$ ensures ϵ-DP [28], Z'_i serves as a privacy mechanism achieving $\frac{n\mathbf{g}'^T_i\mathbf{1}}{1+n^{3/2}\mathbf{g}'^T_1\mathbf{1}}\sqrt{2}$-DP as $R_2, R_3, \cdots, R_{\mathsf{T}}$ are independent unit-variance Laplace random variables.

For $i = 1$, we have that

$$\begin{aligned}
&\sup_{\mathcal{B}\in\mathbb{R}, -1<\lambda<1} \frac{\mathbb{P}\left(A + \left(1 + \frac{1}{n^{3/2}\mathbf{g}'^T_1\mathbf{1}}\right) R_1 \in \mathcal{B}\right)}{\mathbb{P}\left(A + \left(1 + \frac{1}{n^{3/2}\mathbf{g}'^T_1\mathbf{1}}\right) R_1 + \lambda \in \mathcal{B}\right)} \\
= &\sup_{\mathcal{B}\in\mathbb{R}, -\frac{1}{1+\frac{1}{\mathbf{g}'^T_1\mathbf{1}}\frac{1}{n^{3/2}}}<\lambda<\frac{1}{1+\frac{1}{\mathbf{g}'^T_1\mathbf{1}}\frac{1}{n^{3/2}}}} \frac{\mathbb{P}(A + R_1 \in \mathcal{B})}{\mathbb{P}(A + R_1 + \lambda \in \mathcal{B})} \\
&\overset{(a)}{\le} e^{\bar{\epsilon}} + \delta' \le e^{\epsilon},
\end{aligned} \tag{16}$$

where (a) holds as $\lim_{n\to\infty} \frac{1}{1+\frac{1}{n^{3/2}\mathbf{g}'^T_1\mathbf{1}}} = 1$ for any $\delta' > 0$. Hence Z'_1 achieves ϵ-DP.

Since $R_1, R_2, ..., R_{\mathsf{T}}$ are independent, $\mathbf{Z}'$ achieves $\epsilon + \sqrt{2}\sum_{i=2}^{\mathsf{T}} \frac{n\mathbf{g}'^T_i\mathbf{1}}{1+n^{3/2}\mathbf{g}'^T_1\mathbf{1}}$-DP by the composition theorem [6]. As $\lim_{n\to\infty} \frac{n}{n^{3/2}} = 0$, the DP parameter converges to ϵ as $n \to \infty$. For the case with $\mathsf{T} = 1$, the coding scheme still guarantees ϵ-DP as $(A + R_1) + \frac{1}{n^{3/2}} h_i R_1 \approx A + R_1$ for sufficiently large n. Hence we have proved the proposed scheme satisfies T-node ϵ-DP.

C. Accuracy Analysis

Recall that node $i \in [\mathsf{N}]$ computes $\tilde{C}_i = p_A(x_i)p_B(x_i)$, and without loss of generality, we conduct accuracy analysis assuming that node $i \in [\mathsf{T}+1]$ are not erasures or adversaries[4]. The readers can verify that the message vector $\tilde{\mathbf{C}} = \begin{bmatrix} \tilde{C}_1 & \tilde{C}_2 & \cdots & \tilde{C}_{\mathsf{T}+1} \end{bmatrix}^T$ can be rewritten as $\tilde{\mathbf{C}} = \mathbf{V}\begin{bmatrix} m_1 & m_2 & \cdots & m_{\mathsf{T}+1} \end{bmatrix}^T + O\left(\frac{1}{n^2}\right)\mathbf{1}$, where $\mathbf{V}$ is a $\mathsf{N} \times (\mathsf{T}+1)$ Vandermonde matrix with points $\{x_i\}_{i=1}^{\mathsf{N}}$, and $m_1 = (A + R_1)(B + S_1), m_2 =$

[3] Note that we only consider the non-trivial case where $\mathbf{g}'^T_i\mathbf{1} \neq 0$ with $i \in \{2, \cdots, \mathsf{T}\}$. If $\mathbf{g}'^T_i\mathbf{1} = 0$, privacy is well-preserved as only noise remains.

[4] The methods to detect adversaries is detailed in Section III-D.

$\frac{1}{n}\left(S_2(A+R_1)+R_2(B+S_1)\right), \cdots, m_{\mathsf{T}} = \frac{1}{n}(S_{\mathsf{T}}(A+R_1)+R_{\mathsf{T}}(B+S_1))$, $m_{\mathsf{T}+1} = \frac{1}{n^{3/2}}(S_1(A+R_1)+R_1(B+S_1))$.

As the Vandermonde matrix is invertible, the decoder can decompose $\{m_i\}_{i=1}^{\mathsf{T}+1}$ by multiplying $\mathbf{V}^{-1}$. Then the decoder could get $\bar{C}_1 = (A+R_1)(B+S_1) + O\left(\frac{1}{n^2}\right)$. and $\bar{C}_2 = \left(A + \left(1+\frac{1}{n^{3/2}}\right)R_1\right)\left(B+\left(1+\frac{1}{n^{3/2}}\right)S_1\right) + O\left(\frac{1}{n^2}\right)$.

The following lemma is a well-known result from linear mean square estimation theory[29].

Lemma 1: Let X be a random variable with $\mathbb{E}[X] = 0$ and $\mathbb{E}[X^2] = \gamma^2$. Let $\{N_i\}_{i=1}^{m}$ be random noises independent of X, and $\tilde{\mathbf{X}} = \begin{bmatrix}\nu_1 X + N_1 & \cdots & \nu_m X + N_m\end{bmatrix}$, where $\nu_i \in \mathbb{R}$. Then $\inf_{\mathbf{w}} \mathbb{E}[|\mathbf{w}^T \tilde{X} - X|^2] = \frac{\gamma^2}{1+\mathtt{SNR}_a}$, and $\mathtt{SNR}_a = \frac{\det(\mathbf{K}_1)}{\det(\mathbf{K}_2)} - 1.$, where $\mathbf{K}_1$ denotes the covariance matrix of the noisy observation $\tilde{\mathbf{X}}$, and $\mathbf{K}_2$ denotes the covariance matrix of the noise $\{N_i\}_{i=1}^{m}$. Furthermore, there exists $\mathbf{w}^*$ such that the linear mean square error achieves $\frac{\gamma^2}{1+\mathtt{SNR}_a}$.

Since the decoder can estimate the $\tilde{C}$ based on $\bar{C}_1$ and $\bar{C}_2$, the achieved $\mathtt{SNR}_a$ can be bounded as in (17).

$$\begin{aligned}
&\mathtt{SNR}_a \geq \\
&\frac{\begin{vmatrix} \eta^2 + 2\eta\sigma^2\left(1+\frac{1}{n^{3/2}}\right)^2 + \sigma^4\left(1+\frac{1}{n^{3/2}}\right)^4 + O\left(\frac{1}{n^4}\right) & \eta^2 + 2\eta\sigma^2\left(1+\frac{1}{n^{3/2}}\right) + \sigma^4\left(1+\frac{1}{n^{3/2}}\right)^2 + O\left(\frac{1}{n^4}\right) \\ \eta^2 + 2\eta\sigma^2\left(1+\frac{1}{n^{3/2}}\right) + \sigma^4\left(1+\frac{1}{n^{3/2}}\right)^2 + O\left(\frac{1}{n^4}\right) & \eta^2 + 2\eta\sigma^2 + \sigma^4 + O\left(\frac{1}{n^4}\right) \end{vmatrix}}{\begin{vmatrix} 2\eta\sigma^2\left(1+\frac{1}{n^{3/2}}\right)^2 + \sigma^4\left(1+\frac{1}{n^{3/2}}\right)^4 + O\left(\frac{1}{n^4}\right) & 2\eta\sigma^2\left(1+\frac{1}{n^{3/2}}\right) + \sigma^4\left(1+\frac{1}{n^{3/2}}\right)^2 + O\left(\frac{1}{n^4}\right) \\ 2\eta\sigma^2\left(1+\frac{1}{n^{3/2}}\right) + \sigma^4\left(1+\frac{1}{n^{3/2}}\right)^2 + O\left(\frac{1}{n^4}\right) & 2\eta\sigma^2 + \sigma^4 + O\left(\frac{1}{n^4}\right) \end{vmatrix}} - 1 \\
&\overset{(a)}{=} \frac{\eta^2 + 2\eta\sigma^2 + 2\frac{1}{n^{3/2}}\eta\sigma + O(\frac{1}{n^2})}{\sigma^4\left(1+\frac{1}{n^{3/2}}\right)^2 + O(\frac{1}{n^2})} \overset{(b)}{=} \frac{\eta^2}{\sigma^4} + \frac{2\eta}{\sigma^2} + o(n).
\end{aligned} \tag{17}$$

Here (a) holds by omitting $O\left(\frac{1}{n^2}\right)$ term, (b) holds as $\lim_{n\to\infty}\frac{1}{n^{3/2}} = 0$ and $o(n)$ means the term tends to 0 with sufficiently large n. Therefore the lower bound of $\mathtt{SNR}_a$ is derived, i.e.,

$$\mathtt{SNR}_a \geq \frac{\eta^2}{\sigma^4} + \frac{2\eta}{\sigma^2} - \delta', \tag{18}$$

for any $\delta' > 0$ by selecting sufficiently large n. The same result can be easily derived when $\mathsf{T} = 1$.

Combining Lemma 1 and (18), the achievable result in Theorem 1 is proved by substituting $\sigma^2 = (\sigma^*(\epsilon))^2 + \delta'$ with sufficient small δ' as shown in Section III-B.

D. Error Correction Methods

Denote $\mathcal{S}$ as the indices of surviving computation results (non-erasures) with $|\mathcal{S}| = \mathsf{N}-\mathsf{E}$, and $\mathcal{S} = \{s_1, s_2, \cdots, s_{\mathsf{N}-\mathsf{E}}\}$ where $\{s_i\}_{i=1}^{\mathsf{N}-\mathsf{E}}$ denote the indices. Without loss of generality, assume that the set of adversarial nodes that may output erroneous values $\mathcal{A} = \{s_i\}_{i=1}^{\mathsf{A}} \subseteq [\mathsf{N}]$. The computation result from node $i \in \mathsf{N}$, $\tilde{C}_i$ can be expressed as $\tilde{C}_i = p_A(x_i)p_B(x_i)$, i.e., the evaluation of a $2T$-degree polynomial at the point x_i. Correcting A errors of this RS code requires at least $2\mathsf{T}+2\mathsf{A}+1$ [30], while the minimum number of received results is $\mathsf{T}+2\mathsf{A}+1$. However, observe that there are T coefficients in $p_A(x)p_B(x)$ with magnitude $O\left(\frac{1}{n^2}\right)$, which can be neglected as they decay rapidly to zero with sufficiently large n. Hence $\{\tilde{C}_{s_i}\}_{i=1}^{\mathsf{N}-\mathsf{E}}$ can be approximately viewed as a $(\mathsf{N}-\mathsf{E}, \mathsf{T}+1)$ RS code with respect to messages $\{m_i\}_{i=1}^{\mathsf{T}+1}$ and encoding polynomial $P(\cdot)$ with degree T.

We then can utilize the Berlekamp–Welch algorithm [7] adapted to the reals to locate the A errors. Let $E(\cdot)$ denote a monic error locator polynomial of degree A, where $E(x_{s_i}) = 0$ if and only if $i \in [\mathsf{A}]$. Note that $E(\cdot)$ can be represented as $E(x) = e_0 + e_1 x + \cdots + e_{\mathsf{A}-1} x^{\mathsf{A}-1} + x^{\mathsf{A}}$ where $\{e_i\}_{i=0}^{\mathsf{A}-1}$ are A coefficients need to be determined in the decoding process. Let $Q(\cdot)$ denote the product of the error locator polynomial $E(\cdot)$ and message polynomial $P(\cdot)$, and the degree of $Q(\cdot)$ is $\mathsf{T}+\mathsf{A}$. $Q(\cdot)$ can be represented as $Q(x) = q_0 + q_1 x + \cdots + q_{\mathsf{T}+\mathsf{A}} x^{\mathsf{T}+\mathsf{A}}$, where $\{q_i\}_{i=0}^{\mathsf{T}+\mathsf{A}}$ are $\mathsf{T}+\mathsf{A}+1$ coefficients need to be solved in the decoding process. As $O\left(\frac{1}{n^2}\right)$ tends to zero with increasing n, $Y_{s_i} E(x_{s_i}) \approx Q(x_{s_i})$ for any $i \in [\mathsf{N}-\mathsf{A}]$ [7], where the approximate equality arises because the message polynomial is, in fact, of degree $2\mathsf{T}+1$ but with T terms negligible. We can derive the approximate coefficients $\{\tilde{e}_i\}_{i=0}^{\mathsf{A}-1}$ and $\{\tilde{q}_i\}_{i=0}^{\mathsf{T}+\mathsf{A}}$ by solving the linear system,

$$\tilde{\mathbf{C}}\tilde{\mathbf{b}} = \tilde{\mathbf{c}}, \tag{19}$$

where $\tilde{\mathbf{C}} = \begin{bmatrix} Y_{s_1} & \cdots & x_{s_1}^{\mathsf{A}-1} Y_{s_1} & -1 & \cdots & -x_{s_2}^{\mathsf{T}+\mathsf{A}} \\ Y_{s_2} & \cdots & x_{s_2}^{\mathsf{A}-1} Y_{s_2} & -1 & \cdots & -x_{s_2}^{\mathsf{T}+\mathsf{A}} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ Y_{s_{\mathsf{N}-\mathsf{E}}} & \cdots & x_{s_{\mathsf{N}-\mathsf{E}}}^{\mathsf{A}-1} Y_{s_{\mathsf{N}-\mathsf{E}}} & -1 & \cdots & -x_{s_{\mathsf{N}-\mathsf{E}}}^{\mathsf{T}+\mathsf{A}} \end{bmatrix}$, $\tilde{\mathbf{b}} = \begin{bmatrix} \tilde{e}_0 & \cdots & \tilde{e}_{\mathsf{A}-1} & \tilde{q}_0 & \cdots & \tilde{q}_{\mathsf{T}+\mathsf{A}} \end{bmatrix}^T$, and $\tilde{\mathbf{c}} = \begin{bmatrix} -x_{s_1}^{\mathsf{A}} Y_{s_1} & -x_{s_2}^{\mathsf{A}} Y_{s_2} & \cdots & -x_{s_{\mathsf{N}-\mathsf{E}}}^{\mathsf{A}} Y_{s_{\mathsf{N}-\mathsf{E}}} \end{bmatrix}^T$.

The approximate error locater polynomial $\tilde{E}(\cdot)$ can be determined by the coefficients $\{\tilde{e}_i\}_{i=0}^{\mathsf{A}-1}$, and the error node indices can be identified by selecting A evaluation points among $\{x_{s_i}\}_{i=1}^{s_{\mathsf{N}-\mathsf{E}}}$ that minimize $|\tilde{E}(\cdot)|$. The decoding process is considered to be successful if the distortion between the derived and accurate results can be made arbitrarily small. As the polynomial $\tilde{E}(\cdot)$ is the linear combination of $\{e_i\}_{i=0}^{\mathsf{A}-1}$, the error can be located if the distortion between the approximate $\{\tilde{e}_i\}_{i=0}^{\mathsf{A}-1}$ and accurate coefficients $\{e_i\}_{i=0}^{\mathsf{A}-1}$ tends to zero with increasing n. In Appendix A of the extended version of our paper [31], we validate the correctness of the decoding algorithm by establishing bounds on the distortion of the coefficients.

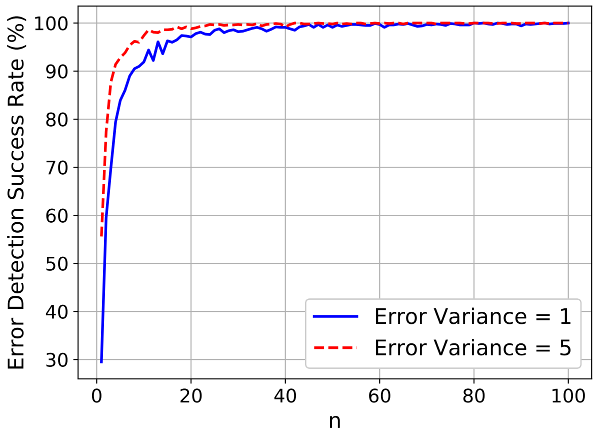

Fig. 1. Comparison of the error detection rate with different error variance.

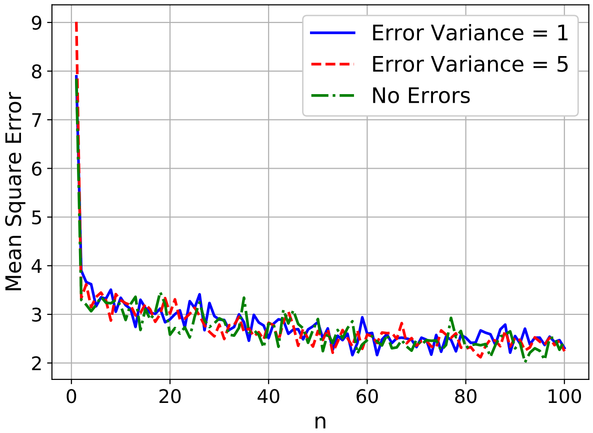

Fig. 2. Comparison of the mean square error with different error variance.

IV. Numerical Simulations

In this section, we conduct numerical simulations to validate the correctness of the proposed coding scheme. The simulations consider the setting with $\mathsf{N} = 16$ nodes, including $\mathsf{T} = 5$ colluding nodes, $\mathsf{E} = 2$ erased nodes, and $\mathsf{A} = 2$ adversarial nodes, satisfying $\mathsf{N} = \mathsf{T} + 2\mathsf{A} + \mathsf{E} + 1$. We let $\eta = 1$, and $\sigma = 0.5$. Among the nodes, E nodes are randomly erased, while $\mathsf{A} = 2$ adversarial nodes introduce errors by adding zero-mean Gaussian noise with variance $\mathbb{E}[\sigma_e^2]$. To analyze the worst-case scenario, we assume that erased nodes and adversarial nodes do not overlap. We select evaluation points $x_i = \cos\left(\frac{(2i-1)\pi}{2\mathsf{N}}\right)$. The simulations aim to demonstrate the system performance with increasing n, and 1000 simulations are conducted for each n to reduce the effects of randomness. Figure 1 illustrates the error detection success rate versus n with error variance $\mathbb{E}[\sigma_e^2] \in \{1, 5\}$. The success detection rates for both error variances converge to nearly 100 % with increasing n, which coincides with the analysis in Section III-D. Besides, the success rate with $\mathbb{E}[\sigma_e^2] = 5$ (the red dotted line) converges more rapidly compared to the success rate with $\mathbb{E}[\sigma_e^2] = 1$ (the blue solid line). This phenomenon, different from that in the finite field, arises because errors of larger magnitude are more readily detected, whereas small errors have a less significant impact on the computation result, even if they remain undetected. Figure 2 compares the mean square error with no adversaries (the green dash-dot line), $\mathbb{E}[\sigma_0^2] = 1$ (the blue solid line) and $\mathbb{E}[\sigma_0^2] = 5$ (the red dotted line). All three lines exhibit similar trends and magnitudes as n increases, showing the effectiveness of the proposed scheme in managing adversarial nodes with varying error magnitudes.

Appendix A

Without loss of generality, we assume that $\mathcal{A} = \{s_1, s_2, \cdots, s_{\mathsf{A}}\}$. We first consider the ideal case by dropping all terms of magnitude $O\left(\frac{1}{n^2}\right)$, and derive a new form of the computation results as follows.

$$\begin{bmatrix} \tilde{C}'_{s_1} \\ \tilde{C}'_{s_2} \\ \vdots \\ \tilde{C}'_{s_{\mathsf{N-E}}} \end{bmatrix} = \begin{bmatrix} 1 & x_{s_1} & x_{s_1}^2 & \cdots & x_1^{\mathsf{T}} \\ 1 & x_{s_2} & x_{s_2}^2 & \cdots & x_{s_2}^{\mathsf{T}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{s_{\mathsf{N-E}}} & x_{s_{\mathsf{N-E}}}^2 & \cdots & x_{s_{\mathsf{N-E}}}^{\mathsf{T}} \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \\ m_3 \\ \vdots \\ m_{\mathsf{T}+1} \end{bmatrix}, \tag{20}$$

which constitutes a $(\mathsf{N-E}, \mathsf{T}+1)$ RS code. We denote the corresponding message polynomial as $p(\cdot)$ of degree T. Similarly, we denote $E(\cdot)$ as a monic error locator polynomial of degree A with coefficients $\{e_i\}_{i=0}^{\mathsf{A}-1}$, and $Q(\cdot)$ of degree $\mathsf{T}+\mathsf{A}$ denote the product of the error locator polynomial $E(\cdot)$ and message polynomial $p(\cdot)$ with $\{q_i\}_{i=0}^{\mathsf{T+A}}$. Note that $Y'_{s_i}E(x_{s_i}) = Q(x_{s_i})$ always achieve for any $i \in [\mathsf{N-E}]$ [7]. As there are $\mathsf{N} - \mathsf{S} = \mathsf{T} + 2\mathsf{A} + 1$ surviving computation results, we could formulate and solve the following linear system.

$$\mathbf{Cb} = \mathbf{c}, \tag{21}$$

$$\mathbf{C} = \begin{bmatrix} Y'_{s_1} & x_{s_1}Y'_{s_1} & \cdots & x_{s_1}^{\mathsf{A}-1}Y'_{s_1} & -1 & -x_{s_1} & \cdots & -x_{s_1}^{\mathsf{T+A}} \\ Y'_{s_2} & x_{s_2}Y'_{s_2} & \cdots & x_{s_2}^{\mathsf{A}-1}Y'_{s_2} & -1 & -x_{s_2} & \cdots & -x_{s_2}^{\mathsf{T+A}} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ Y'_{s_{\mathsf{N-E}}} & x_{s_{\mathsf{N-E}}}Y'_{s_{\mathsf{N-E}}} & \cdots & x_{s_{\mathsf{N-E}}}^{\mathsf{A}-1}Y'_{s_{\mathsf{N-E}}} & -1 & -x_{s_1} & \cdots & -x_{s_{\mathsf{N-E}}}^{\mathsf{T+A}} \end{bmatrix}, \mathbf{b} = \begin{bmatrix} e_0 \\ \vdots \\ e_{\mathsf{A}-1} \\ q_0 \\ \vdots \\ q_{\mathsf{T+A}} \end{bmatrix}, \tilde{\mathbf{c}} = \begin{bmatrix} -x_{s_1}^{\mathsf{A}}Y'_{s_1} \\ -x_{s_2}^{\mathsf{A}}Y'_{s_2} \\ \vdots \\ -x_{s_{\mathsf{N-A}}}^{\mathsf{A}}Y'_{s_{\mathsf{N-A}}} \end{bmatrix}.$$

By solving the above equations, we can determine the coefficients of $E(\cdot)$ and $Q(\cdot)$ and then which allows us to identify the error nodes.

Then we would like to bound the gap between the true coefficients $\mathbf{b}$ and the derived coefficients $\tilde{\mathbf{b}}$. Let $\Delta\mathbf{C} = \begin{bmatrix} O\left(\frac{1}{n^2}\right) & \cdots & O\left(\frac{1}{n^2}\right) & 0 & \cdots & 0 \\ O\left(\frac{1}{n^2}\right) & \cdots & O\left(\frac{1}{n^2}\right) & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ O\left(\frac{1}{n^2}\right) & \cdots & O\left(\frac{1}{n^2}\right) & 0 & \cdots & 0 \end{bmatrix}$, $\Delta\mathbf{c} = \begin{bmatrix} O\left(\frac{1}{n^2}\right) \\ O\left(\frac{1}{n^2}\right) \\ \vdots \\ O\left(\frac{1}{n^2}\right) \end{bmatrix}$, and (21) can be rewritten as,

$$\begin{aligned} (\mathbf{C} + \Delta\mathbf{C})\tilde{\mathbf{b}} &= \mathbf{c} + \Delta\mathbf{c} \\ \mathbf{C}(\tilde{\mathbf{b}} - \mathbf{b}) + \Delta\mathbf{C}\tilde{\mathbf{b}} &= \Delta\mathbf{c} \\ \tilde{\mathbf{b}} - \mathbf{b} &= \mathbf{C}^{-1}(\Delta\mathbf{c} - \Delta\mathbf{C}\tilde{\mathbf{b}}). \end{aligned} \tag{22}$$

By the property of norm, we have

$$\|\tilde{\mathbf{b}} - \mathbf{b}\|_\infty \le \|\mathbf{C}^{-1}\|_\infty \|\Delta\mathbf{c} - \Delta\mathbf{C}\tilde{\mathbf{b}}\|_\infty. \tag{23}$$

For $\Delta\mathbf{c} - \Delta\mathbf{C}\tilde{\mathbf{b}}$, we have $\|\Delta\mathbf{c} - \Delta\mathbf{C}\tilde{\mathbf{b}}\|_\infty = O\left(\frac{1}{n^2}\right)$ based on the magnitude of $\Delta\mathbf{C}$ and $\Delta\mathbf{c}$. As elements in $\mathbf{C}$ and $\mathbf{C}^{-1}$ would not tend to infinity with increasing n, $\|\mathbf{C}^{-1}\|_\infty \|\Delta\mathbf{c} - \Delta\mathbf{C}\tilde{\mathbf{b}}\|_\infty = O\left(\frac{1}{n^2}\right)$. Then the distortion between $\{e_i\}$ and $\{\tilde{e}_i\}$ is upper bounded by an arbitrarily small value, and the correctness of the decoding can be guaranteed as the derived locations will be close to the actual locations.

REFERENCES

[1] V. R. Cadambe, H. Jeong, and F. P. Calmon, "Differentially private secure multiplication: Hiding information in the rubble of noise," in *2023 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2023, pp. 2207–2212.

[2] O. Goldreich, "Secure multi-party computation," *Manuscript. Preliminary version*, vol. 78, no. 110, pp. 1–108, 1998.

[3] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[4] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the society for industrial and applied mathematics*, vol. 8, no. 2, pp. 300–304, 1960.

[5] H. B. McMahan, G. Andrew, U. Erlingsson, S. Chien, I. Mironov, N. Papernot, and P. Kairouz, "A general approach to adding differential privacy to iterative training procedures," *arXiv preprint arXiv:1812.06210*, 2018.

[6] C. Dwork, "Differential privacy," in *International colloquium on automata, languages, and programming*. Springer, 2006, pp. 1–12.

[7] L. R. Welch and E. R. Berlekamp, "Error correction for algebraic block codes," Dec. 30 1986, uS Patent 4,633,470.

[8] 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.

[9] Q. Yu, M. Maddah-Ali, and S. Avestimehr, "Polynomial codes: an optimal design for high-dimensional coded matrix multiplication," *Advances in Neural Information Processing Systems*, vol. 30, 2017.

[10] R. Tandon, Q. Lei, A. G. Dimakis, and N. Karampatziakis, "Gradient coding: Avoiding stragglers in distributed learning," in *International Conference on Machine Learning*. PMLR, 2017, pp. 3368–3376.

[11] K. Wan, H. Sun, M. Ji, and G. Caire, "Distributed linearly separable computation," *IEEE Transactions on Information Theory*, vol. 68, no. 2, pp. 1259–1278, 2021.

[12] A. Khalesi and P. Elia, "Multi-user linearly separable computation: A coding theoretic approach," in *2022 IEEE Information Theory Workshop (ITW)*. IEEE, 2022, pp. 428–433.

[13] 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*. PMLR, 2019, pp. 1215–1225.

[14] 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.

[15] T. Jahani-Nezhad, M. A. Maddah-Ali, S. Li, and G. Caire, "Swiftagg+: Achieving asymptotically optimal communication loads in secure aggregation for federated learning," *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 4, pp. 977–989, 2023.

[16] H. Akbari-Nodehi and M. A. Maddah-Ali, "Secure coded multi-party computation for massive matrix operations," *IEEE Transactions on Information Theory*, vol. 67, no. 4, pp. 2379–2398, 2021.

[17] W.-T. Chang and R. Tandon, "On the capacity of secure distributed matrix multiplication," in *2018 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2018, pp. 1–6.

[18] Z. Jia and S. A. Jafar, "On the capacity of secure distributed batch matrix multiplication," *IEEE Transactions on Information Theory*, vol. 67, no. 11, pp. 7420–7437, 2021.

[19] K. Liang, S. Li, M. Ding, F. Tian, and Y. Wu, "Privacy-preserving coded schemes for multi-server federated learning with straggling links," *IEEE Transactions on Information Forensics and Security*, 2024.

[20] M. Soleymani, M. V. Jamali, and H. Mahdavifar, "Coded computing via binary linear codes: Designs and performance limits," *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 3, pp. 879–892, 2021.

[21] M. Soleymani, H. Mahdavifar, and A. S. Avestimehr, "Analog lagrange coded computing," *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 283–295, 2021.

[22] ——, "Analog secret sharing with applications to private distributed learning," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1893–1904, 2022.

[23] H.-P. Liu, M. Soleymani, and H. Mahdavifar, "Analog multi-party computing: Locally differential private protocols for collaborative computations," *arXiv preprint arXiv:2308.12544*, 2023.

[24] ——, "Differentially private coded computing," in *2023 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2023, pp. 2189–2194.

[25] R. M. Roth, “Analog error-correcting codes,” *IEEE Transactions on Information Theory*, vol. 66, no. 7, pp. 4075–4088, 2020.

[26] A. Jiang, “Analog error-correcting codes: Designs and analysis,” *IEEE Transactions on Information Theory*, 2024.

[27] Q. Geng and P. Viswanath, “The optimal noise-adding mechanism in differential privacy,” *IEEE Transactions on Information Theory*, vol. 62, no. 2, pp. 925–951, 2015.

[28] C. Dwork, F. McSherry, K. Nissim, and A. Smith, “Calibrating noise to sensitivity in private data analysis,” in *Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006. Proceedings 3*. Springer, 2006, pp. 265–284.

[29] H. V. Poor, *An introduction to signal detection and estimation*. Springer Science & Business Media, 2013.

[30] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*. Cambridge university press, 2010.

[31] H. Hu and V. R. Cadambe, “Differentially private secure multiplication with erasures and adversaries,” *https://github.com/Haoyang-Hu/Differentially-Private-Secure-Multiplication-with-Erasures-and-Adversaries*, 2025.