Differentially Private Secure Multiplication with Erasures and Adversaries

Haoyang Hu, Viveck R. Cadambe

Abstract

I. Introduction

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 $[a] \triangleq \{1, \ldots, a\}$. 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 for the distributed computing system 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 $\mathbb{E}[A^2], \mathbb{E}[B^2] \leq \eta$ for some $\eta \geq 0$.

Let each node $i \in [\mathsf{N}]$ store the following encoded version of input A and B in this setting.

$$\tilde{A}_i = a_i A + \tilde{R}_i, \quad \tilde{B}_i = b_i B + \tilde{S}_i, \tag{1}$$

where $\{a_i, b_i\}_{i=1}^{\mathsf{N}}$ are some constant scalars, $\{\tilde{R}_i, \tilde{S}_i\}_{i=1}^{\mathsf{N}}$ are some random variables that are independent with A, B. Without loss of generality, we assume that random variables $A, B, \{\tilde{R}_i, \tilde{S}_i\}_{i=1}^{\mathsf{N}}$ have zero means, and the results of this paper can be readily extended to the case with non-zero means. Each node $i \in [\mathsf{N}]$ then performs the local computation based on encoded data $\tilde{A}_i$ and $\tilde{B}_i$, i.e.,

$$\tilde{C}_i = \tilde{A}_i \tilde{B}_i. \tag{2}$$

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)

After the local computation and message transmission, a decoder collects the output $\{\tilde{C}_i\}_{i=1}^{\mathsf{N}}$ from distributed nodes and then applies a linear decoding function $d : \mathbb{R}^{\mathsf{N}} \to \mathbb{R}$ to estimate the desired multiplication result, i.e.,

$$\tilde{C} = d(\tilde{C}_1, \tilde{C}_2, \cdots, \tilde{C}_{\mathsf{N}}) = \sum_{i=1}^{\mathsf{N}} w_i \tilde{C}_i, \tag{3}$$

where $\{w_i\}_{i=1}^{\mathsf{N}}$ are coefficients of the decoding function d.

A private, resilient, and secure multiplication coding scheme $\mathcal{C}$ includes scalars $\{a_i, b_i\}_{i=1}^{\mathsf{N}}$, the joint distribution of $\{\tilde{R}_i, \tilde{S}_i\}_{i=1}^{\mathsf{N}}$ and the decoding function d. And the coding scheme is specifically designed to satisfy the following criteria:

- **Differential Privacy**: The system must guarantee the differential privacy of the original data A, B even when up to T honest-but-curious nodes collude. The coding scheme is then regarded as T-node differential private, with its formal definition provided in Definition 2.
- **Resiliency**: The decoder must be capable of accurately recovering the multiplication result even if up to E erased nodes fail to transmit their local computation results in time. The coding scheme is then regarded as E-node resilient.
- **Security**: The system must ensure correct recovery of the multiplication result even if up to A nodes act adversarially by sending arbitrary erroneous outputs. The coding scheme is then regarded as A-node secure.

To ensure that the proposed scheme satisfies the worst-case scenario, in the remainder of this paper, we consider the system with E erased nodes and A adversary nodes with non-negative integers E and A. Let $\mathcal{E} \subseteq [\mathsf{N}]$ with $|\mathcal{E}| = \mathsf{E}$ denote the set of erased nodes, and let $\mathcal{A} \subseteq [\mathsf{N}]$ with $|\mathcal{A}| = \mathsf{A}$ denote the set of adversary nodes. We let y_i denote the computation result received by the decoder from node $i \in [\mathsf{N}]$, where

$$y_i = \begin{cases} \tilde{C}_i, & \text{if } i \in [\mathsf{N}]/(\mathcal{E} \cup \mathcal{A}), \\ \text{“e”}, & \text{if } i \in \mathcal{E}, \\ \tilde{C}_i + \varepsilon_i, & \text{if } i \in \mathcal{A}, \end{cases} \tag{4}$$

where “e” represents the message is erased and the decoder receives nothing from node $i \in \mathcal{E}$, and $\varepsilon_i \in \mathbb{R}$ denotes the added error of node $i \in \mathcal{A}$.

We then formally define linear mean square error and T-node ϵ-DP in order to measure the accuracy in recovering desired results and resistance to colluding users of the coding scheme.

Definition 1 (Linear mean square error): For a coding scheme $\mathcal{C}$ consisting of scalars $\{a_i, b_i\}_{i=1}^{\mathsf{N}}$, the joint distribution of $\{\tilde{R}_i, \tilde{S}_i\}_{i=1}^{\mathsf{N}}$ and the decoding function d, the linear mean square error (LMSE) is defined as follows.

$$\texttt{LMSE}(\mathcal{C}) = \mathbb{E}[|\tilde{C} - AB|^2]. \tag{5}$$

Definition 2 (T-node ϵ-DP): A coding scheme $\mathcal{C}$ with scalars $\{a_i, b_i\}_{i=1}^{\mathsf{N}}$, 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,

$$\max\left(\frac{\mathbb{P}\left(\mathbf{Y}_{\mathcal{T}}^{(0)} \in \mathcal{B}\right)}{\mathbb{P}\left(\mathbf{Y}_{\mathcal{T}}^{(1)} \in \mathcal{B}\right)}, \frac{\mathbb{P}\left(\mathbf{Z}_{\mathcal{T}}^{(0)} \in \mathcal{B}\right)}{\mathbb{P}\left(\mathbf{Z}_{\mathcal{T}}^{(1)} \in \mathcal{B}\right)}\right) \leq e^{\epsilon}, \tag{6}$$

where

$$\mathbf{Y}_{\mathcal{T}}^{(\ell)} \triangleq \left[a_{t_1}A_\ell + \tilde{R}_{t_1} \quad a_{t_2}A_\ell + \tilde{R}_{t_2} \quad \cdots \quad a_{i_t}A_\ell + \tilde{R}_{t_\mathsf{T}}\right], \tag{7a}$$

$$\mathbf{Z}_{\mathcal{T}}^{(\ell)} \triangleq \left[b_{t_1}B_\ell + \tilde{S}_{t_1} \quad b_{t_2}B_\ell + \tilde{S}_{t_2} \quad \cdots \quad b_{i_t}B_\ell + \tilde{S}_{t_\mathsf{T}}\right], \tag{7b}$$

with $\ell \in \{0,1\}$, $\mathcal{T} = \{t_1, t_2, \cdots, t_\mathsf{T}\}$.

To later analyze the privacy-accuracy trade-off, we define two signal-to-noise ratio (SNR) metrics: the privacy signal-to-noise ratio $\mathtt{SNR}_p$ and the accuracy signal-to-noise ratio $\mathtt{SNR}_a$.

Definition 3 (Privacy signal-to-noise ratio.): We consider a secure multiplication coding scheme $\mathcal{C}$, and for any set $\mathcal{T} \subseteq [N]$. Let $\mathbf{K}_{\mathcal{T}}^A$ and $\mathbf{K}_{\mathcal{T}}^B$ represent the covariance matrices of $\{\tilde{A}_i\}_{i\in\mathcal{T}}$ and $\{\tilde{B}_i\}_{i\in\mathcal{T}}$ respectively. Let $\mathbf{K}_{\mathcal{T}}^R$ and $\mathbf{K}_{\mathcal{T}}^S$ represent the covariance matrices of $\{\tilde{R}_i\}_{i\in\mathcal{T}}$ and $\{\tilde{S}_i\}_{i\in\mathcal{T}}$ respectively. The privacy signal-to-noise ratios of input A and B, $\mathtt{SNR}_{\mathcal{T}}^A$ and $\mathtt{SNR}_{\mathcal{T}}^B$, are then defined as follows.

$$\mathtt{SNR}_{\mathcal{T}}^A = \frac{\det \mathbf{K}_{\mathcal{T}}^A}{\det \mathbf{K}_{\mathcal{T}}^R} - 1, \tag{8a}$$

$$\mathtt{SNR}_{\mathcal{T}}^B = \frac{\det \mathbf{K}_{\mathcal{T}}^B}{\det \mathbf{K}_{\mathcal{T}}^S} - 1. \tag{8b}$$

For $\mathsf{T} \leq \mathsf{N}$, the T-node privacy SNR of the coding scheme $\mathcal{C}$, $\mathtt{SNR}_p$, is defined as follows.

$$\mathtt{SNR}_p(\mathcal{C}) = \max_{\mathcal{T}\in[\mathsf{N}],|\mathcal{T}|=\mathsf{T}} \max(\mathtt{SNR}_{\mathcal{T}}^A, \mathtt{SNR}_{\mathcal{T}}^B). \tag{9}$$

Definition 4 (Accuracy signal-to-noise ratio.): We consider a secure multiplication coding scheme $\mathcal{C}$. Let $\mathbf{K}_1$ denote the $\mathsf{N}\times\mathsf{N}$ matrix whose (i,j)-th entry is $\mathbb{E}[\tilde{C}_i\tilde{C}_j]$ and $\mathbf{K}_2$ denote the $\mathsf{N}\times\mathsf{N}$ matrix whose (i,j)-th entry is $\mathbb{E}[\tilde{C}_i\tilde{C}_j] - a_ia_jb_ib_j\eta^2$. The accuracy signal-to-noise ratio of the coding scheme $\mathcal{C}$, $\mathtt{SNR}_a$, is then defined as follows.

$$\mathtt{SNR}_a(\mathcal{C}) = \frac{\det(\mathbf{K}_1)}{\det(\mathbf{K}_2)} - 1. \tag{10}$$

The following lemma is a well-known result from linear mean square estimation theory[1] about the linear mean square error and accuracy SNR.

Lemma 1: For a coding scheme $\mathcal{C}$ with accuracy signal-to-noise ratio $\mathtt{SNR}_a(\mathcal{C})$, for inputs A, B satisfying $\mathbb{E}[A^2], \mathbb{E}[B^2] \leq \eta$, we have,

$$\mathtt{LMSE}(\mathcal{C}) \leq \frac{\eta^2}{1 + \mathtt{SNR}_a(\mathcal{C})}, \tag{11}$$

with equality if and only if $\mathbb{E}[A^2] = \mathbb{E}[B^2] = \eta$.

In the remainder of this paper, we omit the dependence on the coding scheme $\mathcal{C}$ in $\mathtt{SNR}_a$ and $\mathtt{SNR}_p$ for simplicity when the relationship is clear from the context.

B. Main Results

The first theorem characterizes the achieved privacy-accuracy trade-off given a certain number of nodes N, number of colluders T, number of erasers S, and number of adversaries A.

Theorem 1: Given positive integers N and non-negative integers $\mathsf{T}, \mathsf{E}, \mathsf{A}$ with $\mathsf{N} \geq \mathsf{T} + \mathsf{E} + 2\mathsf{A} + 1$, there exists a N-node coding scheme $\mathcal{C}$ that guarantees T-node differential privacy, E-node resiliency and A-node security with privacy signal-to-noise ratio $\mathtt{SNR}_p$ and accuracy signal-to-noise ratio $\mathtt{SNR}_a$ satisfying

$$\mathtt{SNR}_a \geq \mathtt{SNR}_p^2 + 2\mathtt{SNR}_p - \delta, \tag{12}$$

for any $\delta > 0$.

Proof 1: See Section III and Section IV.

Remark 1: [2] considers the secure multiplication setting with $\mathsf{T} < \mathsf{N} < 2\mathsf{T} + 1$ and $\mathsf{S} = \mathsf{A} = 0$. [2] states that for any $\mathsf{N} < 2\mathsf{T} + 1$ and any secure coding scheme satisfying T-node ϵ-DP,

$$1 + \mathtt{SNR}_a \leq (1 + \mathtt{SNR}_p)^2. \tag{13}$$

Note that the achievable results in this paper can meet the converse bound arbitrarily closely if $\mathsf{T} + \mathsf{E} + 2\mathsf{A} + 1 \leq \mathsf{N} < 2\mathsf{T} + 1$.

Remark 2: Previous work [2] has demonstrated that the SNR tradeoff in (12) is achieved when $\mathsf{T} < \mathsf{N} < 2\mathsf{T} + 1$[1]. A minimum of $\mathsf{N} = \mathsf{T} + 1$ nodes suffices to achieve this tradeoff, and can arbitrarily closely approach the converse bound, making any additional nodes beyond $\mathsf{T} + 1$ useless. This paper exploits the gain of redundant nodes by introducing a redesigned coding scheme that not only preserves the optimal SNR tradeoff outlined in [2] but also enhances system robustness against erasures and adversaries.

We denote $\sigma^*(\epsilon)$ as the smallest noise variance that achieves single user differential privacy parameter ϵ. The choice of $\sigma^*(\epsilon)$ is specified in [4] as follows.

$$\left(\sigma^*(\epsilon)\right)^2 = \frac{2^{2/3} e^{-2\epsilon/3}(1 + e^{-2\epsilon/3}) + e^{-\epsilon}}{(1 - e^{-\epsilon})^2}. \tag{14}$$

The following theorem presents the relationship between the least mean square error $\mathtt{LMSE}(\mathcal{C})$ and the differential privacy parameter ϵ under the proposed coding scheme $\mathcal{C}$.

Theorem 2: Given positive integers N and non-negative integers $\mathsf{T}, \mathsf{E}, \mathsf{A}$ with $\mathsf{N} \geq \mathsf{T} + \mathsf{E} + 2\mathsf{A} + 1$, there exists a N-node coding scheme $\mathcal{C}$ that guarantees T-node ϵ-DP, E-node resiliency and A-node security with the least mean square error $\mathtt{LMSE}(\mathcal{C})$ satisfying,

$$\mathtt{LMSE}(\mathcal{C}) \leq \frac{\eta^2 \left(\sigma^*(\epsilon)\right)^4}{\left(\eta + \left(\sigma^*(\epsilon)\right)^2\right)^2} + \delta, \tag{15}$$

for any $\delta > 0$.

Proof 2: See Section V.

[1]For $\mathsf{N} \geq 2\mathsf{T} + 1$, the BGW algorithm [3] can ensure perfect privacy and accuracy, i.e., the decoder recovers the results perfectly and any information about the input A and B is not disclosed, resulting in $\mathtt{SNR}_p = 0, \mathtt{SNR}_a = \infty$

III. Proposed Coding Schemes

In this section, we will first present an illustrative example to demonstrate the key idea of the proposed scheme, and then introduce the general form.

A. Illustrative Examples

We consider a distributed computing system with $\mathsf{N} = 5$ nodes and $\mathsf{T} = 2$ colluding nodes. In contrast to [2], $\mathsf{N}-\mathsf{T}-1$ redundant nodes are introduced, enabling the system to handle either two erased nodes or one adversarial node, i.e., $\mathsf{E} = 2, \mathsf{A} = 0$ or $\mathsf{E} = 0, \mathsf{A} = 1$. This subsection primarily focuses on the case with erased nodes, while the scenario involving error correction is further explored in Section IV.

Let $\alpha_1^{(n)}$, $\alpha_2^{(n)}$ be some strictly positive sequences that that approach zero as $n \to \infty$ and satisfy the following condition,

$$\lim_{n\to\infty} \frac{\alpha_1^{(n)}}{\alpha_2^{(n)}} = \lim_{n\to\infty} \alpha_2^{(n)} = \lim_{n\to\infty} \frac{(\alpha_2^{(n)})^2}{\alpha_1^{(n)}} = 0. \tag{16}$$

For instance, one possible choice is $\alpha_1^{(n)} = \frac{1}{n}$ which converges to zero as n increases, and let $\alpha_2^{(n)} = \alpha_1^{(n)} \log\left(\frac{1}{\alpha_1^{(n)}}\right)$.

We select a constant x, whose value will be specified later, and some random variables $\{R_i, S_i\}_{i=1}^2$ satisfying $\mathbb{E}(R_i) = \mathbb{E}(S_i) = 0$ and $\mathbb{E}(R_i^2) = \mathbb{E}(S_i^2) = 1$ for $i \in \{1, 2\}$. Each node then receives the following encoded data.

$$\tilde{A}_1 = A + xR_1 + \alpha_2^{(n)} R_2 + \alpha_1^{(n)} R_1, \quad \tilde{B}_1 = B + xS_1 + \alpha_2^{(n)} S_2 + \alpha_1^{(n)} S_1. \tag{17a}$$

$$\tilde{A}_2 = A + xR_1 + 2\alpha_2^{(n)} R_2 + 4\alpha_1^{(n)} R_1, \quad \tilde{B}_2 = B + xS_1 + 2\alpha_2^{(n)} S_2 + 4\alpha_1^{(n)} S_1. \tag{17b}$$

$$\tilde{A}_3 = A + xR_1 + 3\alpha_2^{(n)} R_2 + 9\alpha_1^{(n)} R_1, \quad \tilde{B}_3 = B + xS_1 + 3\alpha_2^{(n)} S_2 + 9\alpha_1^{(n)} S_1. \tag{17c}$$

$$\tilde{A}_4 = A + xR_1 + 4\alpha_2^{(n)} R_2 + 16\alpha_1^{(n)} R_1, \quad \tilde{B}_4 = B + xS_1 + 4\alpha_2^{(n)} S_2 + 16\alpha_1^{(n)} S_1. \tag{17d}$$

$$\tilde{A}_5 = A + xR_1 + 5\alpha_2^{(n)} R_2 + 25\alpha_1^{(n)} R_1, \quad \tilde{B}_5 = B + xS_1 + 5\alpha_2^{(n)} S_2 + 25\alpha_1^{(n)} S_1. \tag{17e}$$

Based on the local encoded data, node $i \in [5]$ computes $\tilde{C}_i = \tilde{A}_i \tilde{B}_i$ and sends the result to the decoder. We will then analyze the privacy SNR and accuracy SNR of the coding scheme in this example.

1) Privacy Analysis: Due to symmetry, we only focus on analyzing the privacy of A, as the privacy analysis for B follows similarly. To satisfy the privacy requirement with $\mathtt{SNR}_p \approx \frac{\eta}{x^2}$, we choose $x \approx \sqrt{\frac{\eta}{\mathtt{SNR}_p}}$. Let $\mathcal{T} \subseteq [5]$ represent the set of colluding nodes, with $t_1, t_2 \in \mathcal{T}$ denoting the indices of colluding nodes. Using the linear estimator $\beta_{t_1}, \beta_{t_2} \in \mathbb{R}$, the colluders obtain,

$$\begin{aligned}\hat{A} &= \beta_{t_1}\left(A + xR_1 + \alpha_2^{(n)} g_{t_1} R_2 + \alpha_1^{(n)} h_{t_1} R_1\right) + \beta_{t_2}\left(A + xR_1 + \alpha_2^{(n)} g_{t_2} R_2 + \alpha_1^{(n)} h_{t_2} R_1\right) \\ &= \left(\beta_{t_1} + \beta_{t_2}\right) A + \left(\beta_{t_1} + \beta_{t_2}\right) xR_1 + \alpha_1^{(n)}\left(\beta_{t_1} h_{t_1} + \beta_{t_2} h_{t_2}\right) R_1 + \alpha_2^{(n)}\left(\beta_{t_1} g_{t_1} + \beta_{t_2} g_{t_2}\right) R_2,\end{aligned} \tag{18}$$

where $\{g_{t_1}, g_{t_2}\}$ and $\{h_{t_1}, h_{t_2}\}$ are the parameters specified in the above.

The privacy SNR for A is bounded as follows.

$$\begin{aligned}\mathtt{SNR}_{\mathcal{T}}^{A} &= \frac{\left(\beta_{t_1}+\beta_{t_2}\right)^2\eta}{\left(\left(\beta_{t_1}+\beta_{t_2}\right)xR_1+\alpha_1^{(n)}\left(\beta_{t_1}h_{t_1}+\beta_{t_2}h_{t_2}\right)R_1+\alpha_2^{(n)}\left(\beta_{t_1}g_{t_1}+\beta_{t_2}g_{t_2}\right)R_2\right)^2}\\ &\overset{(a)}{=} \frac{\left(\beta_{t_1}+\beta_{t_2}\right)^2\eta}{\left(\left(\beta_{t_1}+\beta_{t_2}\right)x+\alpha_1^{(n)}\left(\beta_{t_1}h_{t_1}+\beta_{t_2}h_{t_2}\right)\right)^2+\left(\alpha_2^{(n)}\right)^2\left(\beta_{t_1}g_{t_1}+\beta_{t_2}g_{t_2}\right)^2}\\ &\overset{(b)}{\leq} \frac{\eta}{x^2+2\alpha_1^{(n)}\frac{\beta_{t_1}h_{t_1}+\beta_{t_2}h_{t_2}}{\beta_{t_1}+\beta_{t_2}}x+\left(\alpha_2^{(n)}\right)^2\frac{\left(\beta_{t_1}g_{t_1}+\beta_{t_2}g_{t_2}\right)^2}{\left(\beta_{t_1}+\beta_{t_2}\right)^2}},\end{aligned} \tag{19}$$

where (a) holds as R_1 and R_2 are independent noise with zero expectation and unit variance, (b) holds by omitting the $O\left(\left(\alpha_1^{(n)}\right)^2\right)$ term. Since $\beta_{t_1}+\beta_{t_2}\neq 0$, we assume that $\beta_{t_1}+\beta_{t_2}=1$[2], i.e., $\beta_{t_2}=1-\beta_{t_1}$. Hence (19) could be rewritten as follows.

$$\begin{aligned}&\mathtt{SNR}_{\mathcal{T}}^{A}\\ &\leq \frac{\eta}{x^2+2\alpha_1^{(n)}\left(\beta_{t_1}(h_{t_1}-h_{t_2})+h_{t_2}\right)x+\left(\alpha_2^{(n)}\right)^2\left(\left(\beta_{t_1}(g_{t_1}-g_{t_2})+g_{t_2}\right)^2\right)}\\ &= \frac{\eta}{\left(\alpha_2^{(n)}\right)^2(g_{t_1}-g_{t_2})^2\beta_{t_1}^2+\left(2\alpha_1^{(n)}x(h_{t_1}-h_{t_2})+2\left(\alpha_2^{(n)}\right)^2(g_{t_1}-g_{t_2})g_{t_2}\right)\beta_{t_1}+x^2+2\alpha_1^{(n)}h_{t_2}x+\left(\alpha_2^{(n)}\right)^2g_{t_2}^2}\\ &\overset{(a)}{=} \frac{\eta}{\left(\alpha_2^{(n)}(g_{t_1}-g_{t_2})\beta_{t_1}+v\right)^2-v^2+x^2+2\alpha_1^{(n)}h_{t_2}x+\left(\alpha_2^{(n)}\right)^2g_{t_2}^2}\\ &\overset{(b)}{\leq} \frac{\eta}{-\frac{\left(\alpha_1^{(n)}\right)^2x^2(h_{t_1}-h_{t_2})^2+2\alpha_1^{(n)}\left(\alpha_2^{(n)}\right)^2x(h_{t_1}-h_{t_2})(g_{t_1}-g_{t_2})g_{t_2}+O\left((\alpha_2^{(n)})^4\right)}{\left(\alpha_2^{(n)}\right)^2(g_{t_1}-g_{t_2})^2}+x^2+2\alpha_1^{(n)}h_{t_2}x+\left(\alpha_2^{(n)}\right)^2g_{t_2}^2}\\ &= \frac{\eta}{x^2-2\alpha_1^{(n)}x(\frac{(h_{t_1}-h_{t_2})g_{t_2}}{g_{t_1}-g_{t_2}}+h_{t_2})+O\left(\frac{\left(\alpha_1^{(n)}\right)^2}{\left(\alpha_2^{(n)}\right)^2}\right)+O\left(\left(\alpha_2^{(n)}\right)^6\right)+O\left(\left(\alpha_2^{(n)}\right)^2\right)}\\ &\overset{(c)}{\approx} \frac{\eta}{x^2-2\alpha_1^{(n)}x(\frac{(h_{t_1}-h_{t_2})g_{t_2}}{g_{t_1}-g_{t_2}}+h_{t_2})}\overset{(d)}{\approx}\frac{\eta}{x^2},\end{aligned} \tag{20}$$

where $v=\frac{\alpha_1^{(n)}x(h_{n_1}-h_{n_2})+\left(\alpha_2^{(n)}\right)^2(g_{n_1}-g_{n_2})g_{n_2}}{\alpha_2^{(n)}(g_{n_1}-g_{n_2})}$, (a) holds by rearranging the formula and the fact that $g_{n_1}\neq g_{n_2}$, (b) holds by selecting appropriate β_1 to let the quadratic term be 0 and the expansion of v^2, (c) holds as $\lim_{n\to\infty}\frac{\alpha_1^{(n)}}{\alpha_2^{(n)}}=\lim_{n\to\infty}\alpha_2^{(n)}=0$, (d) holds as $\lim_{n\to\infty}\alpha_1^{(n)}=0$ and $g_{n_1}\neq g_{n_2}$. Samely, we could derive the upper bound of $\mathtt{SNR}_{\mathcal{T}}^{B}$. Hence the privacy SNR $\mathtt{SNR}_p$ could be bounded as follows.

$$\mathtt{SNR}_p \leq \frac{\eta}{x^2}+\delta, \tag{21}$$

for any $\delta>0$ with sufficiently large n.

2) Accuracy Analysis: In this example, the minimum number of surviving nodes is $\mathsf{N}-\mathsf{E}=3$, meaning that any three computation results from the five nodes are sufficient for the decoder to accurately recover the desired

[2]$\beta_{t_1}+\beta_{t_2}$ cannot be 0, otherwise A is eliminated, making it impossible to infer any information about A. As we perform a linear estimation of A, the estimated parameter $\{\beta_i\}$ can be normalized such that $\beta_{t_1}+\beta_{t_2}=1$. The privacy requirement is proved under this normalization assumption.

result $\tilde{C}$. Let $\mathcal{S}$ denote the set of surviving nodes, with s_1, s_2, s_3 denoting the indices of surviving nodes. The computation results of the surviving node s_i with $i \in [3]$ are as follows.

$$\begin{aligned}\tilde{C}_{s_i} &= (A + xR_1)(B + xS_1) + \alpha_2^{(n)} g_{s_i} \left(S_2(A + xR_1) + R_2(B + xS_1)\right) \\ &\quad + \alpha_1^{(n)} h_{s_i} \left(S_1(A + xR_1) + R_1(B + xS_1)\right) + O\left(\left(\alpha_2^{(n)}\right)^2\right), \end{aligned} \tag{22}$$

where $\{g_{s_i}, h_{s_i}\}_{i=1}^3$ are the parameters specified in the above example. Since any 3×3 matrix $\begin{bmatrix} 1 & g_{s_1} & h_{s_1} \\ 1 & g_{s_2} & h_{s_2} \\ 1 & g_{s_3} & h_{s_3} \end{bmatrix}$ is invertible for any choice of $\mathcal{S} \subset [5]$ in the example, the decoder can derived the following $\bar{C}_1$ based on three surviving results.

$$\bar{C}_1 = (A + xR_1)(B + xS_1) + O\left(\left(\alpha_2^{(n)}\right)^2\right). \tag{23}$$

Similarly, as any 2×2 submatrix of $\begin{bmatrix} 1 & g_{s_1} & h_{s_1} \\ 1 & g_{s_2} & h_{s_2} \end{bmatrix}$ is invertible for any choice of $\mathcal{S} \subset [5]$ in the example, the decoder can derived the following $\bar{C}_2$ based on two surviving results $\tilde{C}_{s_1}, \tilde{C}_{s_2}$.

$$\bar{C}_2 = \left(A + \left(x + c\alpha_1^{(n)}\right) R_1\right)\left(B + \left(x + c\alpha_1^{(n)}\right) S_1\right) + O\left(\left(\alpha_2^{(n)}\right)^2\right), \tag{24}$$

where $c = \frac{g_{s_2} h_{s_1} - g_{s_1} h_{s_2}}{g_{s_2} - g_{s_1}}$ is the derived non-zero coefficient. The decoder can then utilize $\bar{C}_1$ and $\bar{C}_2$ to estimate the product. Consequently, the achieved accuracy SNR can be bounded by using the signal and noise covariance matrices of $\bar{C}_1$ and $\bar{C}_2$, i.e.,

$$\begin{aligned}&\mathtt{SNR}_a \geq \\ &\frac{\begin{vmatrix} \eta^2 + 2\eta\left(x + c\alpha_1^{(n)}\right)^2 + \left(x + c\alpha_1^{(n)}\right)^4 + O\left(\left(\alpha_2^{(n)}\right)^4\right) & \eta^2 + 2\eta x\left(x + c\alpha_1^{(n)}\right) + x^2\left(x + c\alpha_1^{(n)}\right)^2 + O\left(\left(\alpha_2^{(n)}\right)^4\right) \\ \eta^2 + 2\eta x\left(x + c\alpha_1^{(n)}\right) + x^2\left(x + c\alpha_1^{(n)}\right)^2 + O\left(\left(\alpha_2^{(n)}\right)^4\right) & \eta^2 + 2\eta x^2 + x^4 + O\left(\left(\alpha_2^{(n)}\right)^4\right) \end{vmatrix}}{\begin{vmatrix} 2\eta\left(x + c\alpha_1^{(n)}\right)^2 + \left(x + c\alpha_1^{(n)}\right)^4 + O\left(\left(\alpha_2^{(n)}\right)^4\right) & 2\eta x\left(x + c\alpha_1^{(n)}\right) + x^2\left(x + c\alpha_1^{(n)}\right)^2 + O\left(\left(\alpha_2^{(n)}\right)^4\right) \\ 2\eta x\left(x + c\alpha_1^{(n)}\right) + x^2\left(x + c\alpha_1^{(n)}\right)^2 + O\left(\left(\alpha_2^{(n)}\right)^4\right) & 2\eta x^2 + x^4 + O\left(\left(\alpha_2^{(n)}\right)^4\right) \end{vmatrix}} - 1 \\ &\overset{(a)}{\approx} \frac{\eta^2 + 2\eta x^2 + 2c\alpha_1^{(n)}\eta x}{x^2\left(x + c\alpha_1^{(n)}\right)^2} \\ &\overset{(b)}{\approx} \frac{\eta^2}{x^4} + \frac{2\eta}{x^2}, \end{aligned} \tag{25}$$

where (a) holds by omitting $O\left(\left(\alpha_1^{(n)}\right)^2\right)$ terms and $O\left(\left(\alpha_2^{(n)}\right)^2\right)$ terms, (b) holds as $\lim_{n\to\infty} \alpha_1^{(n)} = 0$.

Hence the accuracy SNR $\mathtt{SNR}_a$ could be bounded as,

$$\mathtt{SNR}_a \geq \frac{\eta^2}{x^4} + \frac{2\eta}{x^2} + \delta, \tag{26}$$

for any $\delta > 0$ with sufficiently large n.

Based on (21) and (26), the relationship between privacy SNR and accuracy SNR in this example satisfies the achievable result in Theorem 1.

B. General Schemes

In this subsection, we will introduce the general form of the proposed coding scheme.

For $\mathsf{T} > 1$, non-negative integers E, A, and $\mathsf{N} \geq \mathsf{T}+\mathsf{E}+2\mathsf{A}+1$, let $\{f_0, f_1, \cdots, f_{\mathsf{T}}\}$ be a set of polynomial basis of dimension T. In addition, we require $f_0 = 1$. For instance, the set can be the monomial basis $\{1, a, a^2, \cdots, a^{\mathsf{T}}\}$. Selecting N distinct non-zero real numbers $\{a_i\}_{i=1}^{\mathsf{N}}$, a $\mathsf{N} \times (\mathsf{T}+1)$ encoding matrix can be formed as follows.

$$\mathbf{M} = \begin{bmatrix} 1 & f_1(a_1) & f_2(a_1) & \cdots & f_{\mathsf{T}}(a_1) \\ 1 & f_1(a_2) & f_2(a_2) & \cdots & f_{\mathsf{T}}(a_2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & f_1(a_{\mathsf{N}}) & f_2(a_{\mathsf{N}}) & \cdots & f_{\mathsf{T}}(a_{\mathsf{N}}) \end{bmatrix}_{\mathsf{N}\times(\mathsf{T}+1)}, \tag{27}$$

Note that 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 based on properties of the basis. If $\{f_i\}_{i=0}^{\mathsf{T}}$ represents the monomial basis, the encoding matrix will take the form of a Vandermonde matrix of size $\mathsf{N}\times(\mathsf{T}+1)$. The encoding process can be expressed as follows,

$$\begin{bmatrix} \tilde{A}_1 & \tilde{A}_2 & \cdots & \tilde{A}_{\mathsf{N}-1} & \tilde{A}_{\mathsf{N}} \end{bmatrix}^T = \mathbf{M} \begin{bmatrix} A + xR_1 & \alpha_2^{(n)} R_2 & \cdots & \alpha_2^{(n)} R_{\mathsf{T}} & \alpha_1^{(n)} R_1 \end{bmatrix}^T \tag{28a}$$

$$\begin{bmatrix} \tilde{B}_1 & \tilde{B}_2 & \cdots & \tilde{B}_{\mathsf{N}-1} & \tilde{B}_{\mathsf{N}} \end{bmatrix}^T = \mathbf{M} \begin{bmatrix} B + xS_1 & \alpha_2^{(n)} S_2 & \cdots & \alpha_2^{(n)} S_{\mathsf{T}} & \alpha_1^{(n)} S_1 \end{bmatrix}^T, \tag{28b}$$

where $x \approx \sqrt{\frac{\eta}{\mathtt{SNR}_p}}$ and $\{R_i, S_i\}_{i=1}^{\mathsf{T}}$ are statistically independent random variables with zero mean unit variance. The choice of $\{R_i, S_i\}_{i=1}^{\mathsf{T}}$ will specified in Section V to guarantee the differential privacy. Let $\mathbf{M} = \begin{bmatrix} \mathbf{1} & \mathbf{G} & \mathbf{h} \end{bmatrix}$, where $\mathbf{1}$ and $\mathbf{h} = \begin{bmatrix} h_1 & h_2 & \cdots & h_{\mathsf{N}} \end{bmatrix}$ denotes column vectors, and $\mathbf{G} = \begin{bmatrix} \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_{\mathsf{N}} \end{bmatrix}^T$ represents a matrix of size $\mathsf{N}\times(\mathsf{T}-1)$,

The received coded data of node $i \in \mathsf{N}$ can be rewritten as follows.

$$\tilde{A}_i = (A + xR_1) + \alpha_2^{(n)} \begin{bmatrix} R_2 & R_3 & \cdots & R_{\mathsf{T}} \end{bmatrix} \mathbf{g}_i + \alpha_1^{(n)} h_i R_1, \tag{29a}$$

$$\tilde{B}_i = (B + xS_1) + \alpha_2^{(n)} \begin{bmatrix} S_2 & S_3 & \cdots & S_{\mathsf{T}} \end{bmatrix} \mathbf{g}_i + \alpha_1^{(n)} h_i S_1. \tag{29b}$$

Note that the noise added to the original data can be interpreted as a superposition of three layers:

- **First Layer**: This noise, denoted as xR_1 or xS_1, has a magnitude of $O(1)$ and is designed to ensure differential privacy by selecting an appropriate constant x.
- **Second Layer**: This layer, with magnitude of $O\left(\alpha_2^{(n)}\right)$, ensures T-node privacy by making the input data inaccessible for any T colluding nodes.
- **Third Layer**: Correlated with the first layer, this noise has a magnitude of $O\left(\alpha_1^{(n)}\right)$. After the decoder removes the second layer of noise, this layer can be obtained and utilized to improve accuracy.

For the case with $\mathsf{T} = 1$, there is no second layer of noise, and the received coded data of node $i \in \mathsf{N}$ can be represented as follows.

$$\tilde{A}_i = (A + xR_1) + \alpha_1^{(n)} h_i R_1, \quad \tilde{B}_i = (B + xS_1) + \alpha_1^{(n)} h_i S_1. \tag{30}$$

Each node $i \in [\mathsf{N}]$ computes $\tilde{C}_i = \tilde{A}_i \tilde{B}_i$, and then transmit the result to the decoder. After receiving $\mathsf{N}-\mathsf{E}$ computation results, the decoder identifies at most A errors utilizing techniques described in Section IV, and obtains

$\mathsf{N}-\mathsf{E}-2\mathsf{A}$ accurate computation results. Since $\mathsf{N} \geq \mathsf{T}+\mathsf{E}+2\mathsf{A}+1$, the decoder is guaranteed to get at least $\mathsf{T}+1$ accurate computation result. The decoder then applies the linear decoding function d to estimate the product of A and B.

In the following, we will analyze the privacy SNR where at most T nodes collude, as well as the accuracy SNR where at least $\mathsf{T}+1$ accurate computation results are available to the decoder.

1) Privacy Analysis: Considering any set of colluding nodes $\mathcal{T} \subseteq [N]$ with $|\mathcal{T}| = \mathsf{T}$, we aim to prove that

$$\mathtt{SNR}_p = \max_{\mathcal{T}\in[\mathsf{N}],|\mathcal{T}|=\mathsf{T}} \max\left(\mathtt{SNR}_{\mathcal{T}}^{A}, \mathtt{SNR}_{\mathcal{T}}^{B}\right) \leq \frac{\eta}{x^2}+\delta, \tag{31}$$

for any $\delta > 0$ when n is sufficiently large. Because of the symmetry of the coding scheme, it suffices only to analyze the privacy SNR of input A, and prove that $\mathtt{SNR}_{\mathcal{T}}^{A} \leq \frac{\eta}{x^2}+\delta$ for any $\mathcal{T} \subseteq \mathsf{N}$.

For the set of colluding nodes $\mathcal{T}$, we let $\{t_i\}_{i=1}^{\mathsf{T}}$ denote the indices of colluding nodes, i.e., $\mathcal{T} = \{t_1, t_2, ..., t_{\mathsf{T}}\}$. Let $\mathbf{h}_{\mathcal{T}} = \begin{bmatrix} h_{t_1} & h_{t_2} & \cdots & h_{t_{\mathsf{T}}} \end{bmatrix}^T$. Applying a linear estimator with a set of coefficients $\boldsymbol{\beta}_{\mathcal{T}} = \begin{bmatrix} \beta_{t_1} & \beta_{t_2} & \cdots & \beta_{t_{\mathsf{T}}} \end{bmatrix}^T$, the colluders get

$$\hat{A} = \mathbf{1}^T\boldsymbol{\beta}_{\mathcal{T}}A + \left(\mathbf{1}^T\boldsymbol{\beta}_{\mathcal{T}}x + \alpha_1^{(n)}\boldsymbol{\beta}_{\mathcal{T}}^T\mathbf{h}_{\mathcal{T}}\right)R_1 + \alpha_2^{(n)}\begin{bmatrix} R_2 & R_3 & \cdots & R_{\mathsf{T}} \end{bmatrix}\left(\sum_{i\in\mathsf{T}}\beta_{t_i}\mathbf{g}_{t_i}\right). \tag{32}$$

The privacy SNR for A is bounded as follows.

$$\begin{aligned}
\mathtt{SNR}_{\mathcal{T}}^{(A)} &= \frac{\left(\mathbf{1}^T\boldsymbol{\beta}_{\mathcal{T}}\right)^2\eta}{\left(\left(\mathbf{1}^T\boldsymbol{\beta}_{\mathcal{T}}x + \alpha_1^{(n)}\boldsymbol{\beta}_{\mathcal{T}}^T\mathbf{h}_{\mathcal{T}}\right)R_1 + \alpha_2^{(n)}\begin{bmatrix} R_2 & R_3 & \cdots & R_{\mathsf{T}} \end{bmatrix}\left(\sum_{i\in\mathsf{T}}\beta_{t_i}\mathbf{g}_{t_i}\right)\right)^2} \\
&\overset{(a)}{=} \frac{\left(\mathbf{1}^T\boldsymbol{\beta}_{\mathcal{T}}\right)^2\eta}{\left(\mathbf{1}^T\boldsymbol{\beta}_{\mathcal{T}}x + \alpha_1^{(n)}\boldsymbol{\beta}_{\mathcal{T}}^T\mathbf{h}_{\mathcal{T}}\right)^2 + \left(\alpha_2^{(n)}\right)^2\left\|\sum_{i\in\mathsf{T}}\beta_{t_i}\mathbf{g}_{t_i}\right\|^2} \\
&\overset{(b)}{\leq} \frac{\eta}{x^2 + 2\alpha_1^{(n)}\frac{\boldsymbol{\beta}_{\mathcal{T}}^T\mathbf{h}_{\mathcal{T}}}{\mathbf{1}^T\boldsymbol{\beta}_{\mathcal{T}}}x + \frac{\left(\alpha_2^{(n)}\right)^2\left\|\sum_{i\in\mathsf{T}}\beta_{t_i}\mathbf{g}_{t_i}\right\|^2}{\left(\mathbf{1}^T\boldsymbol{\beta}_{\mathcal{T}}\right)^2}},
\end{aligned} \tag{33}$$

where (a) holds as $\{R_i\}_{i\in[\mathsf{T}]}$ are independent noise with zero expectation and unit variance, (b) holds by omitting the $O\left(\left(\alpha_1^{(n)}\right)^2\right)$ term. Since the colluders aim to estimate A based on the collected linear combinations of A, it must hold that $\mathbf{1}^T\boldsymbol{\beta}_{\mathcal{T}} \neq 0$ to prevent A from being eliminated. As the colluders perform a linear estimation of A, we can normalize the linear estimation parameters such that $\mathbf{1}^T\boldsymbol{\beta}_{\mathcal{T}} = 1$, and then prove the privacy requirement is satisfied under this normalized assumption. Let $\mathbf{G}_{\mathcal{T}} = \begin{bmatrix} \mathbf{g}_{t_1} & \mathbf{g}_{t_2} & \cdots & \mathbf{g}_{t_{\mathsf{T}}} \end{bmatrix}^T$ of size $\mathsf{T}\times(\mathsf{T}-1)$, and hence (33) could be rewritten as follows.

$$\begin{aligned}
\mathtt{SNR}_{\mathcal{T}}^{(A)} &\leq \frac{\eta}{x^2 + \left(\alpha_2^{(n)}\right)^2\boldsymbol{\beta}_{\mathcal{T}}^T\mathbf{G}_{\mathcal{T}}\mathbf{G}_{\mathcal{T}}^T\boldsymbol{\beta}_{\mathcal{T}} + 2\alpha_1^{(n)}\boldsymbol{\beta}_{\mathcal{T}}^T\mathbf{h}_{\mathcal{T}}x} \\
&\overset{(a)}{=} \frac{\eta}{x^2 + \left(\alpha_2^{(n)}\right)^2\boldsymbol{\beta}_{\mathcal{T}}^T\left(\mathbf{G}_{\mathcal{T}}\mathbf{G}_{\mathcal{T}}^T + \gamma\mathbf{1}\mathbf{1}^T\right)\boldsymbol{\beta}_{\mathcal{T}} + 2\alpha_1^{(n)}\boldsymbol{\beta}_{\mathcal{T}}^T\mathbf{h}_{\mathcal{T}}x - \left(\alpha_2^{(n)}\right)^2\gamma\boldsymbol{\beta}_{\mathcal{T}}^T\mathbf{1}\mathbf{1}^T\boldsymbol{\beta}_{\mathcal{T}}} \\
&\overset{(b)}{=} \frac{\eta}{x^2 + \left(\alpha_2^{(n)}\right)^2\boldsymbol{\beta}_{\mathcal{T}}^T\left(\mathbf{G}_{\mathcal{T}}\mathbf{G}_{\mathcal{T}}^T + \gamma\mathbf{1}\mathbf{1}^T\right)\boldsymbol{\beta}_{\mathcal{T}} + 2\alpha_1^{(n)}\boldsymbol{\beta}_{\mathcal{T}}^T\mathbf{h}_{\mathcal{T}}x - \left(\alpha_2^{(n)}\right)^2\gamma},
\end{aligned} \tag{34}$$

where (a) holds by adding and subtracting the quadratic term $\left(\alpha_2^{(n)}\right)^2\gamma\boldsymbol{\beta}_{\mathcal{T}}^T\mathbf{1}\mathbf{1}^T\boldsymbol{\beta}_{\mathcal{T}}$ with some positive constant $\gamma \in \mathbb{R}^+$, (b) holds by the normalization assumption that $\mathbf{1}^T\boldsymbol{\beta}_{\mathcal{T}} = 1$.

We let the quadratic parameter matrix $\mathbf{Q}_{\mathcal{T}} = \mathbf{G}_{\mathcal{T}}\mathbf{G}_{\mathcal{T}}^T + \gamma \mathbf{1}\mathbf{1}^T$ of size $\mathsf{T}\times\mathsf{T}$, and assume that it is singular, i.e., there exists at least one non-zero vector $\nu \in \mathbb{R}^{\mathsf{T}}$ such that $\nu^T\mathbf{Q}_{\mathcal{T}}\nu = \nu^T\mathbf{G}_{\mathcal{T}}\mathbf{G}_{\mathcal{T}}^T\nu + \gamma\nu^T\mathbf{1}\mathbf{1}^T\nu = 0$. Since $\nu^T\mathbf{G}_{\mathcal{T}}\mathbf{G}_{\mathcal{T}}^T\nu$ and $\gamma\nu^T\mathbf{1}\mathbf{1}^T\nu$ are both non-negative, it follows that $\nu^T\mathbf{G}_{\mathcal{T}}\mathbf{G}_{\mathcal{T}}^T\nu = \gamma\nu^T\mathbf{1}\mathbf{1}^T\nu = 0$, i.e., $\nu^T\mathbf{G}_{\mathcal{T}} = \mathbf{1}^T\nu = 0$. Recall that the coding scheme requires that every $\mathsf{T}\times\mathsf{T}$ submatrix of $\mathbf{M}$ is invertible, the matrix $\begin{bmatrix}\mathbf{1} & \mathbf{G}_{\mathcal{T}}\end{bmatrix}$ of size $\mathsf{T}\times\mathsf{T}$ is also full rank. Hence the only vector ν that simultaneously satisfies $\nu^T\mathbf{G}_{\mathcal{T}} = \mathbf{1}^T\nu = 0$ is the zero vector, which contradicts the initial assumption that ν is non-zero. Hence the matrix $\mathbf{Q}_{\mathcal{T}}$ is invertible and positive-definite.

For the function $f(\boldsymbol{\beta}_{\mathcal{T}}) = \left(\alpha_2^{(n)}\right)^2 \boldsymbol{\beta}_{\mathcal{T}}^T\left(\mathbf{G}_{\mathcal{T}}\mathbf{G}_{\mathcal{T}}^T + \gamma\mathbf{1}\mathbf{1}^T\right)\boldsymbol{\beta}_{\mathcal{T}} + 2\alpha_1^{(n)}\boldsymbol{\beta}_{\mathcal{T}}^T\mathbf{h}_{\mathcal{T}}x$, it can be lower bounded while selecting $\boldsymbol{\beta}_{\mathcal{T}}^*$ such that $\nabla f(\boldsymbol{\beta}_{\mathcal{T}}^*) = 0$. Let $\nabla f(\boldsymbol{\beta}_{\mathcal{T}}) = 2\left(\alpha_2^{(n)}\right)^2\mathbf{Q}_{\mathcal{T}}\boldsymbol{\beta}_{\mathcal{T}} + 2\alpha_1^{(n)}\mathbf{h}_{\mathcal{T}}x = 0$,it follows that $\boldsymbol{\beta}_{\mathcal{T}}^* = -\frac{\alpha_1^{(n)}x}{\left(\alpha_2^{(n)}\right)^2}\mathbf{Q}_{\mathcal{T}}^{-1}\mathbf{h}_{\mathcal{T}}$. Substituting ${\beta_{\mathcal{T}}}^*$ in (34), the privacy SNR can be upper bounded as follows.

$$\begin{aligned}
\mathtt{SNR}_{\mathcal{T}}^A &\leq \frac{\eta}{x^2 - \frac{\left(\alpha_1^{(n)}\right)^2x^2}{\left(\alpha_2^{(n)}\right)^2}\mathbf{h}_{\mathcal{T}}^T\mathbf{Q}_{\mathcal{T}}^{-1}\mathbf{h}_{\mathcal{T}} - \left(\alpha_2^{(n)}\right)^2\gamma} \\
&\overset{(a)}{=} \frac{\eta}{x^2 + O\left(\frac{\left(\alpha_1^{(n)}\right)^2}{\left(\alpha_2^{(n)}\right)^2}\right) + O\left(\left(\alpha_2^{(n)}\right)^2\right)} \\
&\overset{(b)}{\approx} \frac{\eta}{x^2},
\end{aligned} \tag{35}$$

where (a) holds as $\mathbf{h}_{\mathcal{T}}^T\mathbf{Q}_{\mathcal{T}}^{-1}\mathbf{h}_{\mathcal{T}}$ cannot tend to be infinity for given encoding matrix $\mathbf{M}$, (b) holds as $\lim_{n\to\infty}\frac{\alpha_1^{(n)}}{\alpha_2^{(n)}} = \lim_{n\to\infty}\alpha_2^{(n)} = 0$. Applying a similar privacy analysis to B, we have that, for any $\delta > 0$ with sufficiently large n,

$$\mathtt{SNR}_p = \max_{\mathcal{T}\in[\mathsf{N}],|\mathcal{T}|=\mathsf{T}} \max(\mathtt{SNR}_{\mathcal{T}}^A, \mathtt{SNR}_{\mathcal{T}}^B) \leq \frac{\eta}{x^2} + \delta. \tag{36}$$

2) Accuracy Analysis: Based on encoded data $\tilde{A}_i$ and $\tilde{B}_i$, node $i \in [\mathsf{N}]$ computes,

$$\begin{aligned}
\tilde{C}_i = (A + xR_1)(B + xS_1) + \alpha_2^{(n)}\Big((A + (x+\alpha_1^{(n)})h_iR_1)\begin{bmatrix}S_2 & \cdots & S_t\end{bmatrix} \\
+(B + (x+\alpha_1^{(n)}h_i)S_1)\begin{bmatrix}R_2 & \cdots & R_t\end{bmatrix}\Big)\mathbf{g}_i + \alpha_1^{(n)}h_i\left(S_1(A + R_1x) + R_1(B + S_1x)\right) + O\left((\alpha_2^{(n)})^2\right).
\end{aligned} \tag{37}$$

As any $(\mathsf{T}+1)\times(\mathsf{T}+1)$ submatrix of the encoding matrix $\mathbf{M} = \begin{bmatrix}\mathbf{1} & \mathbf{G} & \mathbf{h}\end{bmatrix}_{\mathsf{N}\times(\mathsf{T}+1)}$ is full rank, based on the computation results from any surviving node set $\mathcal{S} \subseteq [\mathsf{N}]$ of size $|\mathcal{S}| = \mathsf{T}+1$, there exists a set of scalars to cancel all $O\left(\alpha_1^{(n)}\right)$ and $O\left(\alpha_2^{(n)}\right)$ terms. Hence the decoder can get the following $\bar{C}_1$.

$$\bar{C}_1 = (A + xR_1)(B + xS_1) + O\left((\alpha_2^{(n)})^2\right). \tag{38}$$

Similarly, as any $\mathsf{T}\times\mathsf{T}$ submatrix of the encoding matrix $\mathbf{M}$ is invertible, the decoder can obtain the following $\bar{C}_2$ based on the surviving computation results.

$$\bar{C}_2 = \left(A + \left(x + c\alpha_1^{(n)}\right)R_1\right)\left(B + \left(x + c\alpha_1^{(n)}\right)S_1\right) + O\left(\left(\alpha_2^{(n)}\right)^2\right), \tag{39}$$

where c is the calculated non-zero coefficient. Note that c must be non-zero as any $(\mathsf{T}-1)\times(\mathsf{T}-1)$ submatrix of the encoding matrix $\mathbf{M}$ is invertible. As the decoder can estimate the $C=AB$ based on $\bar{C}_1$ and $\bar{C}_2$, the achieved accuracy SNR can be bounded as follows.

$$
\begin{aligned}
&\mathtt{SNR}_a \geq \\
&\frac{\begin{vmatrix} \eta^2+2\eta\left(x+c\alpha_1^{(n)}\right)^2+\left(x+c\alpha_1^{(n)}\right)^4+O\left(\left(\alpha_2^{(n)}\right)^4\right) & \eta^2+2\eta x\left(x+c\alpha_1^{(n)}\right)+x^2\left(x+c\alpha_1^{(n)}\right)^2+O\left(\left(\alpha_2^{(n)}\right)^4\right) \\ \eta^2+2\eta x\left(x+c\alpha_1^{(n)}\right)+x^2\left(x+c\alpha_1^{(n)}\right)^2+O\left(\left(\alpha_2^{(n)}\right)^4\right) & \eta^2+2\eta x^2+x^4+O\left(\left(\alpha_2^{(n)}\right)^4\right) \end{vmatrix}}{\begin{vmatrix} 2\eta\left(x+c\alpha_1^{(n)}\right)^2+\left(x+c\alpha_1^{(n)}\right)^4+O\left(\left(\alpha_2^{(n)}\right)^4\right) & 2\eta x\left(x+c\alpha_1^{(n)}\right)+x^2\left(x+c\alpha_1^{(n)}\right)^2+O\left(\left(\alpha_2^{(n)}\right)^4\right) \\ 2\eta x\left(x+c\alpha_1^{(n)}\right)+x^2\left(x+c\alpha_1^{(n)}\right)^2+O\left(\left(\alpha_2^{(n)}\right)^4\right) & 2\eta x^2+x^4+O\left(\left(\alpha_2^{(n)}\right)^4\right) \end{vmatrix}}-1 \\
&\overset{(a)}{\approx} \frac{\eta^2+2\eta x^2+2c\alpha_1^{(n)}\eta x}{x^2\left(x+c\alpha_1^{(n)}\right)^2} \\
&\overset{(b)}{\approx} \frac{\eta^2}{x^4}+\frac{2\eta}{x^2},
\end{aligned} \tag{40}
$$

where (a) holds by omitting $O\left(\left(\alpha_2^{(n)}\right)^2\right)$ term, (b) holds as $\lim_{n\to\infty}\alpha_1^{(n)}=0$. Therefore the lower bound of the accuracy SNR $\mathtt{SNR}_a$ is derived, i.e.,

$$
\mathtt{SNR}_a \geq \frac{\eta^2}{x^4}+\frac{2\eta}{x^2}-\delta, \tag{41}
$$

for any $\delta>0$ by selecting sufficiently large n.

Combining (36) and (41), the achievable result in Theorem 1 is proved.

IV. Error Correction Methods

In this section, we will introduce the error correction method for the proposed coding scheme. We first provide an example of error correction, and then present the general form of the decoding algorithm.

A. Illustrative Examples

Consider the example shown in Section III-A with $\mathsf{N}=5$ distributed nodes, $\mathsf{T}=2$ colluding nodes. As $\mathsf{N}-\mathsf{T}-1=2$, the decoder could locate $\mathsf{A}=1$ error. Using the proposed coding scheme, each node $i\in[5]$ receives the following encoded $\{\tilde{A}_i,\tilde{B}_i\}$,

$$
\begin{bmatrix}\tilde{A}_1\\ \tilde{A}_2\\ \tilde{A}_3\\ \tilde{A}_4\\ \tilde{A}_5\end{bmatrix}=\begin{bmatrix}1&1&1\\1&2&2^2\\1&3&3^2\\1&4&4^2\\1&5&5^2\end{bmatrix}\begin{bmatrix}A+xR_1\\ \alpha_2^{(n)}R_2\\ \alpha_1^{(n)}R_1\end{bmatrix},\quad \begin{bmatrix}\tilde{B}_1\\ \tilde{B}_2\\ \tilde{B}_3\\ \tilde{B}_4\\ \tilde{B}_5\end{bmatrix}=\begin{bmatrix}1&1&1\\1&2&2^2\\1&3&3^2\\1&4&4^2\\1&5&5^2\end{bmatrix}\begin{bmatrix}B+xS_1\\ \alpha_2^{(n)}S_2\\ \alpha_1^{(n)}S_1\end{bmatrix}, \tag{42}
$$

where we select monomial basis $\{1,a,a^2\}$ and evaluation points $a_1=1$, $a_2=2$, $a_3=3$, $a_4=4$, $a_5=5$.

After the local computation, each node $i \in [5]$ gets $\tilde{C}_i$ as follows.

$$\begin{bmatrix} \tilde{C}_1 \\ \tilde{C}_2 \\ \tilde{C}_3 \\ \tilde{C}_4 \\ \tilde{C}_5 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 2^2 & 2^3 & 2^4 \\ 1 & 3 & 3^2 & 3^3 & 3^4 \\ 1 & 4 & 4^2 & 4^3 & 4^4 \\ 1 & 5 & 5^2 & 5^3 & 5^4 \end{bmatrix} \begin{bmatrix} (A+xR_1)(B+xS_1) \\ \alpha_2^{(n)} S_2(A+xR_1) + \alpha_2^{(n)} R_2(B+xS_1) \\ \alpha_1^{(n)} S_1(A+xR_1) + \alpha_1^{(n)} R_1(B+xS_1) + \left(\alpha_2^{(n)}\right)^2 R_2 S_2 \\ \alpha_1^{(n)}\alpha_2^{(n)} R_2 S_1 + \alpha_1^{(n)}\alpha_2^{(n)} R_1 S_2 \\ \left(\alpha_1^{(n)}\right)^2 R_1 S_1 \end{bmatrix}. \tag{43}$$

We let $m_1 = (A+xR_1)(B+xS_1), m_2 = \alpha_2^{(n)} S_2(A+xR_1) + \alpha_2^{(n)} R_2(B+xS_1), m_3 = \alpha_1^{(n)} S_1(A+xR_1) + \alpha_1^{(n)} R_1(B+xS_1)$. Note that based on the accuracy analysis in Section III, $\{m_i\}_{i=1}^3$ are the message sufficient for the decoder to achieve the target accuracy. Without loss of generality, we assume that node 1 is the adversary node, i.e, $y_1 = \tilde{C}_1 + \varepsilon_1$, where ε_1 is the error value of node 1, and $y_i = \tilde{C}_i$ for other node i.

We omit all the terms related to $O\left(\left(\alpha_2^{(n)}\right)^2\right)$ as they tend to zeros with increasing n, and derive a new form of the computation results $\{\tilde{C}_i'\}_{i=1}^5$ as follows.

$$\begin{bmatrix} \tilde{C}_1' \\ \tilde{C}_2' \\ \tilde{C}_3' \\ \tilde{C}_4' \\ \tilde{C}_5' \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 2^2 \\ 1 & 3 & 3^2 \\ 1 & 4 & 4^2 \\ 1 & 5 & 5^2 \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix}. \tag{44}$$

This expression shows that each $\{\tilde{C}_i'\}$ can be interpreted as the evaluation of a 2-degree function $P(a) = \sum_{i=1}^3 m_i a^{i-1}$ at the evaluation point a_i, i.e., $P(a_i)$. Hence the set $\{\tilde{C}_i'\}_{i=1}^N$ forms a $(5,3)$ Reed–Solomon (RS) code with an error-correcting capability of $\mathsf{A} = 1$ [5]. In the following, we will use the modified Berlekamp–Welch algorithm [6] to locate $\mathsf{A} = 1$ error.

Let $E(\cdot)$ represent a monic error locator polynomial of degree $\mathsf{A} = 1$ satisfying $E(a_1) = 0$, i.e., the error polynomial takes 0 at the evaluation point corresponding to the adverarial node. In this example, we have that $E(a) = e_0 + a$ with the polynomial coefficient $e_0 = -a_1$. Let $Q(\cdot)$ denote the product of the error locator polynomial $E(\cdot)$ and message polynomial $P(\cdot)$. The degree of $Q(\cdot)$ is $\mathsf{T} + \mathsf{A} = 3$, where $Q(a) = q_0 + q_1 a + q_2 a^2 + q_3 a^3$ with polynomial coefficients $\{q_i\}_{i=0}^3$. Note that the coefficients of both $E(\cdot)$ and $Q(\cdot)$, i.e., e_0 and $\{q_i\}_{i=0}^3$, are initially unknown to the decoder. If the decoder can determine these coefficients, it will successfully identify the error location. Let $\{y_i'\}_{i=1}^5$ denote the received message related to the above coding scheme, $y_1' = \tilde{C}_1' + \varepsilon_1$ and $y_i' = \tilde{C}_i'$ for other choices of i. Due to the fact that $y_i' E(a_i) = Q(a_i)$ for any $i \in [\mathsf{N}]$ [6], we could formulate the following linear system under the assumption that node 1 sends an erroneous result.

$$\mathbf{C}\mathbf{b} = \mathbf{c}, \tag{45}$$

where $\mathbf{C} = \begin{bmatrix} y_1' & -1 & -1 & -1 & -1 \\ y_2' & -1 & -2 & -4 & -8 \\ y_3' & -1 & -3 & -9 & -27 \\ y_4' & -1 & -4 & -16 & -64 \\ y_5' & -1 & -5 & -25 & -125 \end{bmatrix}$, $\mathbf{b} = \begin{bmatrix} e_0 \\ q_0 \\ q_1 \\ q_2 \\ q_3 \end{bmatrix}$, $\mathbf{c} = \begin{bmatrix} -y_1' \\ -2y_2' \\ -3y_3' \\ -4y_4' \\ -5y_5' \end{bmatrix}$.

By solving the above linear system $\mathbf{b} = \mathbf{C}^{-1}\mathbf{c}$, we obtain $e_0 = -1$, indicating that the error occurs at node 1. However, in the actual decoding process, the received message still includes terms with magnitude $O\left(\left(\alpha_2^{(n)}\right)^2\right)$ even though $O\left(\left(\alpha_2^{(n)}\right)^2\right)$ approaches to 0 with increasing n, i.e,

$$y_1 = y_1' + O\left(\left(\alpha_2^{(n)}\right)^2\right), \quad y_2 = y_2' + O\left(\left(\alpha_2^{(n)}\right)^2\right), y_3 = y_3' + O\left(\left(\alpha_2^{(n)}\right)^2\right),$$
$$y_4 = y_4' + O\left(\left(\alpha_2^{(n)}\right)^2\right), \quad y_5 = y_5' + O\left(\left(\alpha_2^{(n)}\right)^2\right).$$

Based on the above received messages, we could formulate the following modified linear system and get the approximate error location $\tilde{e}_0$.

$$\tilde{\mathbf{C}}\tilde{\mathbf{b}} = \tilde{\mathbf{c}}, \tag{46}$$

where $\tilde{\mathbf{C}} = \begin{bmatrix} y_1 & -1 & -1 & -1 & -1 \\ y_2 & -1 & -2 & -4 & -8 \\ y_3 & -1 & -3 & -9 & -27 \\ y_4 & -1 & -4 & -16 & -64 \\ y_5 & -1 & -5 & -25 & -125 \end{bmatrix}$, $\tilde{\mathbf{b}} = \begin{bmatrix} \tilde{e}_0 \\ \tilde{q}_0 \\ \tilde{q}_1 \\ \tilde{q}_2 \\ \tilde{q}_3 \end{bmatrix}$, $\tilde{\mathbf{c}} = \begin{bmatrix} -y_1 \\ -2y_2 \\ -3y_3 \\ -4y_4 \\ -5y_5 \end{bmatrix}$

After obtaining the coefficient $\tilde{e_0}$, the decoder could evaluate the polynomial $\tilde{E}(a) = \tilde{e}_0 + a$ at evaluation points $\{a_i\}_{i=1}^5$, and choose the a_i that minimize $\tilde{E}(a)$. The decoder can successfully locate the error if the solution $\tilde{e_0}$ closely approximates the true error location e_0, where e_0 is derived via (45). To ensure the error is located correctly, we require,

$$|\tilde{e}_0 - e_0| < \frac{1}{2} \min_{i,j \in [\mathsf{N}]} |a_i - a_j|. \tag{47}$$

In this specific example, we have $|\tilde{e}_0 - e_0| < \frac{1}{2}$.

We let $\Delta\mathbf{C}$ denote the difference between $\mathbf{C}$ and $\tilde{\mathbf{C}}$ and $\Delta\mathbf{c}$ denote the difference between $\mathbf{c}$ and $\tilde{\mathbf{c}}$. Hence (46) can be rewritten as follows.

$$\begin{aligned} (\mathbf{C} + \Delta\mathbf{C})\tilde{\mathbf{y}} &= \mathbf{c} + \Delta\mathbf{c} \\ \mathbf{C}(\tilde{\mathbf{y}} - \mathbf{y}) + \Delta\mathbf{C}\tilde{\mathbf{y}} &\overset{(a)}{=} \Delta\mathbf{c} \\ \tilde{\mathbf{y}} - \mathbf{y} &= \mathbf{C}^{-1}(\Delta\mathbf{c} - \Delta\mathbf{C}\tilde{\mathbf{y}}) \end{aligned} \tag{48}$$

where $\Delta\mathbf{C} = \begin{bmatrix} O\left(\left(\alpha_2^{(n)}\right)^2\right) & 0 & 0 & 0 \\ O\left(\left(\alpha_2^{(n)}\right)^2\right) & 0 & 0 & 0 \\ O\left(\left(\alpha_2^{(n)}\right)^2\right) & 0 & 0 & 0 \\ O\left(\left(\alpha_2^{(n)}\right)^2\right) & 0 & 0 & 0 \\ O\left(\left(\alpha_2^{(n)}\right)^2\right) & 0 & 0 & 0 \end{bmatrix}$ and $\Delta\mathbf{c} = \begin{bmatrix} O\left(\left(\alpha_2^{(n)}\right)^2\right) \\ O\left(\left(\alpha_2^{(n)}\right)^2\right) \\ O\left(\left(\alpha_2^{(n)}\right)^2\right) \\ O\left(\left(\alpha_2^{(n)}\right)^2\right) \\ O\left(\left(\alpha_2^{(n)}\right)^2\right) \end{bmatrix}$, (a) holds by substracting (45). By the property of the matrix norm, we have

$$\|\tilde{\mathbf{y}} - \mathbf{y}\|_\infty \leq \|\mathbf{C}^{-1}\|_\infty \|\Delta\mathbf{c} - \Delta\mathbf{C}\tilde{\mathbf{y}}\|_\infty. \tag{49}$$

Due to the fact that $\|\Delta\mathbf{C}\|_\infty = O\left((\alpha_2^{(n)})^2\right)$ and $\|\Delta\mathbf{c}\|_\infty = O\left((\alpha_2^{(n)})^2\right)$, we have that $\|\Delta\mathbf{c} - \Delta\mathbf{C}\tilde{\mathbf{y}}\|_\infty = O\left((\alpha_2^{(n)})^2\right)$. Calculating $\mathbf{C}^{-1}$, it follows that $\|\mathbf{C}^{-1}\|_\infty = \max\left(49, |\frac{16}{\varepsilon_1}|\right)$. Hence $\|\mathbf{C}^{-1}\|_\infty \|\Delta\mathbf{c} - \Delta\mathbf{C}\tilde{\mathbf{y}}\|_\infty$ will tends to zero with sufficiently large n. The distortion between the true error location e_0 and $\tilde{e}_0$ is upper bounded by an arbitrarily small value, so the correctness of the decoding can be guaranteed.

B. General Error Correction Algorithms

In this subsection, we present the general error correction algorithm with N distributed nodes, T colluding nodes, E erased nodes, and A adversary nodes, satisfying $\mathsf{N} = \mathsf{T} + \mathsf{E} + 2\mathsf{A} + 1$. Denote $\mathcal{S}$ as the indices of surviving computation results 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. Based on the coding scheme described in Section III, we have

$$\begin{bmatrix} \tilde{A}_{s_1} \\ \tilde{A}_{s_2} \\ \vdots \\ \tilde{A}_{s_{\mathsf{N}-\mathsf{E}}} \end{bmatrix} = \begin{bmatrix} 1 & f_1(a_{s_1}) & \cdots & f_{\mathsf{T}}(a_{s_1}) \\ 1 & f_1(a_{s_2}) & \cdots & f_{\mathsf{T}}(a_{s_2}) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & f_1(a_{s_{\mathsf{N}-\mathsf{E}}}) & \cdots & f_{\mathsf{T}}(a_{s_{\mathsf{N}-\mathsf{E}}}) \end{bmatrix} \begin{bmatrix} A + xR_1 \\ \alpha_2^{(n)} R_2 \\ \vdots \\ \alpha_2^{(n)} R_{\mathsf{T}} \\ \alpha_1^{(n)} R_1 \end{bmatrix}, \tag{50a}$$

$$\begin{bmatrix} \tilde{B}_{s_1} \\ \tilde{B}_{s_2} \\ \vdots \\ \tilde{B}_{s_{\mathsf{N}-\mathsf{E}}} \end{bmatrix} = \begin{bmatrix} 1 & f_1(a_{s_1}) & \cdots & f_{\mathsf{T}}(a_{s_1}) \\ 1 & f_1(a_{s_2}) & \cdots & f_{\mathsf{T}}(a_{s_2}) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & f_1(a_{s_{\mathsf{N}-\mathsf{E}}}) & \cdots & f_{\mathsf{T}}(a_{s_{\mathsf{N}-\mathsf{E}}}) \end{bmatrix} \begin{bmatrix} B + xS_1 \\ \alpha_2^{(n)} S_2 \\ \vdots \\ \alpha_2^{(n)} S_{\mathsf{T}} \\ \alpha_1^{(n)} S_1 \end{bmatrix}, \tag{50b}$$

where $\{a_{s_i}\}_{i=1}^{s_{\mathsf{N}-\mathsf{E}}}$ denote distinct evaluation points. Note the encoding process is based on a polynomial of dimension $\mathsf{T}+1$, and each node $i \in \mathcal{S}$ gets the encoded data by evaluating the polynomial using a_i. Following the local

computations performed across the distributed nodes, each node obtains:

$$\begin{bmatrix} \tilde{C}_{s_1} \\ \tilde{C}_{s_2} \\ \vdots \\ \tilde{C}_{s_{\mathsf{N}-\mathsf{E}}} \end{bmatrix} = \begin{bmatrix} 1 & f_1(a_{s_1}) & f_2(a_{s_1}) & \cdots & f_{\mathsf{T}}(a_{s_1}) & f_1(a_{s_1})f_2(a_{s_1}) & \cdots & f_{\mathsf{T}}(a_{s_1})f_{\mathsf{T}}(a_{s_1}) \\ 1 & f_1(a_{s_2}) & f_2(a_{s_2}) & \cdots & f_{\mathsf{T}}(a_{s_2}) & f_1(a_{s_2})f_2(a_{s_2}) & \cdots & f_{\mathsf{T}}(a_{s_2})f_{\mathsf{T}}(a_{s_2}) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 1 & f_1(a_{s_{\mathsf{N}-\mathsf{E}}}) & f_2(a_{s_{\mathsf{N}-\mathsf{E}}}) & \cdots & f_{\mathsf{T}}(a_{s_{\mathsf{N}-\mathsf{E}}}) & f_1(a_{s_{\mathsf{N}-\mathsf{E}}})f_2(a_{s_{\mathsf{N}-\mathsf{E}}}) & \cdots & f_{\mathsf{T}}(a_{s_{\mathsf{N}-\mathsf{E}}})f_{\mathsf{T}}(a_{s_{\mathsf{N}-\mathsf{E}}}) \end{bmatrix}$$
$$\begin{bmatrix} (A+xR_1)(B+xS_1) \\ \alpha_2^{(n)}S_2(A+xR_1)+\alpha_2^{(n)}R_2(B+xS_1) \\ \alpha_2^{(n)}S_3(A+xR_1)+\alpha_2^{(n)}R_3(B+xS_1)+O\left(\left(\alpha_2^{(n)}\right)^2\right) \\ \vdots \\ \alpha_1^{(n)}S_1(A+xR_1)+\alpha_1^{(n)}R_1(B+xS_1)+O\left(\left(\alpha_2^{(n)}\right)^2\right) \\ O\left(\left(\alpha_2^{(n)}\right)^2\right) \\ \vdots \\ O\left(\left(\alpha_2^{(n)}\right)^2\right) \end{bmatrix}. \tag{51}$$

We denote the sets of message $\{m_i\}_{i=1}^{\mathsf{T}+1}$ as $m_1 = (A+xR_1)(B+xS_1), m_2 = \alpha_2^{(n)}S_2(A+xR_1)+\alpha_2^{(n)}R_2(B+xS_1), \cdots, m_{\mathsf{T}+1} = \alpha_1^{(n)}S_1(A+xR_1)+\alpha_1^{(n)}R_1(B+xS_1)$. Note that m_1 and $m_{\mathsf{T}+1}$ are the only information needed by the decoder that can achieve the target accuracy SNR as shown in Section III. We could overlook $O\left(\left(\alpha_2^{(n)}\right)^2\right)$ terms as they are arbitrary small with sufficiently large n. As the basises set $\{1, f_1, f_2, \cdots, f_{\mathsf{T}}\}$ spans the polynomial space of dimension T, hence the $\{\tilde{C}_{s_i}\}_{i=1}^{\mathsf{N}-\mathsf{E}}$ 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 let $\mathcal{A} \subseteq [N]$ denote the set of error nodes with $|\mathcal{A}| = \mathsf{A}$. Without loss of generality, we assume that $\mathcal{A} = \{s_i\}_{i=1}^{\mathsf{A}}$. Hence for $i \in [\mathsf{A}]$

$$y_{s_i} = \tilde{C}_{s_i} + \varepsilon_{s_i}, \tag{52}$$

where $\{\varepsilon_{s_i}\}_{i=1}^{\mathsf{A}}$ denote error values, and $y_{s_i} = \tilde{C}_{s_i}$ with $i \in [\mathsf{A}]$.

We then can utilize the modified Berlekamp–Welch algorithm [6] to locate the A errors. Let $\tilde{E}(\cdot)$ denote a monic error locator polynomial of degree A, where $\tilde{E}(a_{s_i}) = 0$ if and only if $i \in |\mathsf{A}|$. Note that $\tilde{E}(\cdot)$ can be represented as $\tilde{E}(a) = \tilde{e}_0 + \tilde{e}_1 a + \cdots + \tilde{e}_{\mathsf{A}-1}a^{\mathsf{A}-1} + a^{\mathsf{A}}$ where $\{\tilde{e}_i\}_{i=0}^{\mathsf{A}-1}$ are A coefficients need to be determined in the decoding process. Let $\tilde{Q}(\cdot)$ denote the product of the error locator polynomial $\tilde{E}(\cdot)$ and message polynomial $P(\cdot)$, and the degree of $\tilde{Q}(\cdot)$ is $\mathsf{T}+\mathsf{A}$. $\tilde{Q}(\cdot)$ can be represented as $Q(a) = \tilde{q}_0 + \tilde{q}_1 a + \cdots \tilde{q}_{\mathsf{T}+\mathsf{A}}a^{\mathsf{T}+\mathsf{A}}$, where $\{q_i\}_{i=0}^{\mathsf{T}+\mathsf{A}}$ are $\mathsf{T}+\mathsf{A}+1$ coefficients need to be solved in the decoding process. Note that $\tilde{y}'_{s_i}\tilde{E}(a_{s_i}) \approx \tilde{Q}(a_{s_i})$ for any $i \in [\mathsf{N}-\mathsf{A}]$ [6], due to the fact that $O\left(\left(\alpha_2^{(n)}\right)^2\right)$ tends to zero with increasing n. We can only derive the following coefficients $\{\tilde{e}_i\}_{i=0}^{\mathsf{A}-1}$ and $\{\tilde{q}_i\}_{i=0}^{\mathsf{T}+\mathsf{A}}$ by solving the following linear system.

$$\tilde{\mathbf{C}}\tilde{\mathbf{b}} = \tilde{\mathbf{c}}, \tag{53}$$

$$\text{where } \tilde{\mathbf{C}} = \begin{bmatrix} y_{s_1} & ay_{s_1} & \cdots & a^{\mathsf{A}-1}y_{s_1} & -1 & -a_{s_1} & \cdots & -a_{s_2}^{\mathsf{T}+\mathsf{A}} \\ y_{s_2} & ay_{s_2} & \cdots & a^{\mathsf{A}-1}y_{s_2} & -1 & -a_{s_2} & \cdots & -a_{s_2}^{\mathsf{T}+\mathsf{A}} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ y_{s_{\mathsf{N}-\mathsf{A}}} & ay_{s_{\mathsf{N}-\mathsf{A}}} & \cdots & a^{\mathsf{A}-1}y_{s_{\mathsf{N}-\mathsf{A}}} & -1 & -a_{s_{\mathsf{N}-\mathsf{A}}} & \cdots & -a_{s_{\mathsf{N}-\mathsf{A}}}^{\mathsf{T}+\mathsf{A}} \end{bmatrix}, \tilde{\mathbf{b}} = \begin{bmatrix} \tilde{e}_0 \\ \vdots \\ \tilde{e}_{\mathsf{A}-1} \\ \tilde{q}_0 \\ \vdots \\ \tilde{q}_{\mathsf{T}+\mathsf{A}} \end{bmatrix}, \tilde{\mathbf{c}} = \begin{bmatrix} -a_{s_1}^{\mathsf{A}} y_{s_1} \\ -a_{s_2}^{\mathsf{A}} y_{s_2} \\ \vdots \\ -a_{s_{\mathsf{N}-\mathsf{A}}}^{\mathsf{A}} y_{s_{\mathsf{N}-\mathsf{A}}} \end{bmatrix}.$$

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

C. Distortion Analysis

Without loss 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 $O\left(\left(\alpha_2^{(n)}\right)^2\right)$, and derive a new form of the computation results as follows.

$$\begin{bmatrix} \tilde{C}'_{s_1} \\ \tilde{C}'_{s_2} \\ \vdots \\ \tilde{C}'_{s_{\mathsf{N}-\mathsf{E}}} \end{bmatrix} = \begin{bmatrix} 1 & a_{s_1} & a_{s_1}^2 & \cdots & a_1^{\mathsf{T}+1} \\ 1 & a_{s_2} & a_{s_2}^2 & \cdots & a_{s_2}^{\mathsf{T}+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_{s_{\mathsf{N}-\mathsf{E}}} & a_{s_{\mathsf{N}-\mathsf{E}}}^2 & \cdots & a_{s_{\mathsf{N}-\mathsf{E}}}^{\mathsf{T}+1} \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \\ m_3 \\ \vdots \\ m_{\mathsf{T}+1} \end{bmatrix}, \tag{54}$$

which constitutes a $(\mathsf{N}-\mathsf{E}, \mathsf{T}+1)$ 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 $\tilde{E}(\cdot)$ and message polynomial $p(\cdot)$ with $\{q_i\}_{i=0}^{\mathsf{T}+\mathsf{A}}$. Note that $y'_{s_i}E(a_{s_i}) = Q(a_{s_i})$ always achieve for any $i \in [\mathsf{N}-\mathsf{A}]$ [6]. 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.

$$\mathbf{C}\mathbf{b} = \mathbf{c}, \tag{55}$$

$$\text{where } \mathbf{C} = \begin{bmatrix} y'_{s_1} & ay'_{s_1} & \cdots & a^{\mathsf{A}-1}y'_{s_1} & -1 & -a_{s_1} & \cdots & -a_{s_2}^{\mathsf{T}+\mathsf{A}} \\ y'_{s_2} & ay'_{s_2} & \cdots & a^{\mathsf{A}-1}y'_{s_2} & -1 & -a_{s_2} & \cdots & -a_{s_2}^{\mathsf{T}+\mathsf{A}} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ y'_{s_{\mathsf{N}-\mathsf{A}}} & ay'_{s_{\mathsf{N}-\mathsf{A}}} & \cdots & a^{\mathsf{A}-1}y'_{s_{\mathsf{N}-\mathsf{A}}} & -1 & -a_{s_{\mathsf{N}-\mathsf{A}}} & \cdots & -a_{s_{\mathsf{N}-\mathsf{A}}}^{\mathsf{T}+\mathsf{A}} \end{bmatrix}, \mathbf{b} = \begin{bmatrix} e_0 \\ \vdots \\ e_{\mathsf{A}-1} \\ q_0 \\ \vdots \\ q_{\mathsf{T}+\mathsf{A}} \end{bmatrix}, \mathbf{c} = \begin{bmatrix} -a_{s_1}^{\mathsf{A}} y'_{s_1} \\ -a_{s_2}^{\mathsf{A}} y'_{s_2} \\ \vdots \\ -a_{s_{\mathsf{N}-\mathsf{A}}}^{\mathsf{A}} y'_{s_{\mathsf{N}-\mathsf{A}}} \end{bmatrix}.$$

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 $\Delta\mathbf{C} = \begin{bmatrix} O\left(\left(\alpha_2^{(n)}\right)^2\right) & 0 & \cdots & 0 \\ O\left(\left(\alpha_2^{(n)}\right)^2\right) & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ O\left(\left(\alpha_2^{(n)}\right)^2\right) & 0 & \cdots & 0 \end{bmatrix}$, $\Delta\mathbf{c} = \begin{bmatrix} O\left(\left(\alpha_2^{(n)}\right)^2\right) \\ O\left(\left(\alpha_2^{(n)}\right)^2\right) \\ \vdots \\ O\left(\left(\alpha_2^{(n)}\right)^2\right) \end{bmatrix}$, and (55) can be rewritten as,

$$(\mathbf{C}+\Delta\mathbf{C})\tilde{\mathbf{b}} = \mathbf{c}+\Delta\mathbf{c}$$

$$\mathbf{C}(\tilde{\mathbf{b}}-\mathbf{b}) + \Delta\mathbf{C}\tilde{\mathbf{b}} = \Delta\mathbf{c}$$

$$\tilde{\mathbf{b}}-\mathbf{b} = \mathbf{C}^{-1}(\Delta\mathbf{c}-\Delta\mathbf{C}\tilde{\mathbf{b}}). \tag{56}$$

By the property of norm, we have

$$\|\tilde{\mathbf{b}}-\mathbf{b}\|_\infty \le \|\mathbf{C}^{-1}\|_\infty \|\Delta\mathbf{c}-\Delta\mathbf{C}\tilde{\mathbf{b}}\|_\infty. \tag{57}$$

For $\Delta\mathbf{c}-\Delta\mathbf{C}\tilde{\mathbf{b}}$, we have $\|\Delta\mathbf{c}-\Delta\mathbf{C}\tilde{\mathbf{b}}\|_\infty = O\left(\left(\alpha_2^{(n)}\right)^2\right)$ based on the magnitude of $\Delta\mathbf{C}$ and $\Delta\mathbf{c}$. For the matrix $\mathbf{C}$, we could perform the following linear transformation.

$$\mathbf{C} = \begin{bmatrix} y'_{s_1} & -1 & -a_{s_1} & -a_{s_1}^2 & \cdots & -a_{s_1}^{\mathsf{T}+2\mathsf{A}-1} \\ y'_{s_2} & -1 & -a_{s_2} & -a_{s_2}^2 & \cdots & -a_{s_2}^{\mathsf{T}+2\mathsf{A}-1} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ y'_{s_{\mathsf{N}-\mathsf{E}}} & -1 & -a_{s_{\mathsf{N}-\mathsf{E}}} & -a_{s_{\mathsf{N}-\mathsf{E}}}^2 & \cdots & -a_{s_{\mathsf{N}-\mathsf{E}}}^{\mathsf{T}+2\mathsf{A}-1} \end{bmatrix} \longrightarrow \begin{bmatrix} \varepsilon_{s_1} & -1 & \cdots & \cdots & -a_{s_1}^{\mathsf{T}+2\mathsf{A}-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \varepsilon_{s_{\mathsf{A}}} & -1 & \cdots & \cdots & -a_{s_{\mathsf{A}}}^{\mathsf{T}+2\mathsf{A}-1} \\ 0 & -1 & \cdots & \cdots & -a_{s_{\mathsf{A}}+1}^{\mathsf{T}+2\mathsf{A}-1} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & -1 & \cdots & \cdots & -a_{s_{\mathsf{N}-\mathsf{E}}}^{\mathsf{T}+2\mathsf{A}-1} \end{bmatrix} \tag{58}$$

The determinant $\det\mathbf{C}$ can be represented as $\det\mathbf{C} = \sum_{i\in[\mathsf{A}]} c_i\varepsilon_{s_i}$, where $\{c_i\}$ denote some calculated constants. Then the inverse matrix could be derived as $\mathbf{C}^{-1} = \frac{1}{\det(\mathbf{C})}\text{adj}(\mathbf{C}) = \frac{1}{\sum_{i\in[\mathsf{A}]} c_i\varepsilon_{s_i}}\text{adj}(\mathbf{C})$, where $\text{adj}(\mathbf{C})$ denotes the adjugate matrix and each element would not tend to infinity with increasing n. Hence $\|\mathbf{C}^{-1}\|_\infty\|\Delta\mathbf{c}-\Delta\mathbf{C}\tilde{\mathbf{b}}\|_\infty = O\left(\left(\alpha_2^{(n)}\right)^2\right)$. 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.

V. Differential Privacy Analysis

In this section, we analyze the differential privacy properties of the proposed scheme detailed in Section III. Similarly, due to the symmetry of the proposed coding scheme, it suffices to demonstrate that the input data A satisfies T-node ϵ-DP with a fixed DP parameter $\epsilon \ge 0$ and describe the design of additive noise $\{R_i\}_{i=1}^{\mathsf{T}}$.

For a given DP parameter ϵ, let $x = \sigma^*(\epsilon) + \delta'$ with some $\delta' > 0$, where σ^* is defined as (14). Supposing that this choice of x can ensure T-node ϵ-DP of A, we first discuss the upper bound of the estimated error, i.e., $\mathtt{LMSE}$. Recall that in Section III, x is set as $x \approx \sqrt{\frac{\eta}{\mathtt{SNR}_p}}$, which leads to $\mathtt{SNR}_p \approx \frac{\eta}{(\sigma^*(\epsilon))^2}$ by selecting δ' arbitrarily small. As Theorem 1 suggests that $1+\mathtt{SNR}_a \approx (1+\mathtt{SNR}_p)^2$, it follows that

$$\mathtt{SNR}_a \approx \frac{\eta^2 + 2\eta\left(\sigma^*(\epsilon)\right)^2}{\left(\sigma^*(\epsilon)\right)^4}. \tag{59}$$

Together with Lemma 1, it follows that

$$\texttt{LMSE}(\mathcal{C}) \leq \frac{\eta^2 \left(\sigma^*(\epsilon)\right)^4}{\left(\eta + \left(\sigma^*(\epsilon)\right)^2\right)^2} + \delta, \tag{60}$$

for any $\delta > 0$. Hence Theorem 2 is proved under the assumption that T-node ϵ-DP is satisfied, and in the following, we will prove the T-node ϵ-DP of A by selecting $x = \sigma^*(\epsilon) + \delta'$.

For a fixed value of parameter x, let ϵ^* be defined as,

$$\epsilon^* = \inf_{Z, \mathbb{E}[Z^2] \geq 1} \sup_{\mathcal{B}, A_0, A_1 \in \mathbb{R}, |A_0 - A_1| \leq 1} \ln\left(\frac{\mathbb{P}(A_0 + xZ)}{\mathbb{P}(A_1 + xZ)}\right), \tag{61}$$

where $Z \in \mathbb{R}$. Note that the noise variance $\mathbb{E}[x^2 Z^2] = x^2$ 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 (14)) and $\mathbb{E}[x^2 Z^2] > (\sigma^*(\epsilon))^2$, it follows that $\epsilon^* < \epsilon$. Let $Z^*(\bar{\epsilon})$ be the random variable that achieves the DP parameter $\bar{\epsilon}$ with $\epsilon^* < \bar{\epsilon} < \epsilon$, and let the added noise R_1 follow the same distribution as $Z^*(\bar{\epsilon})$. We then let noise $R_2, R_3, \cdots, R_{\mathsf{N}}$ be independent unit variance Laplace random variables independent of R_1. By this construction, we have

$$\sup_{\mathcal{B} \in \mathbb{R}, -1 < \lambda < 1} \frac{\mathbb{P}(A + xR_1 \in \mathcal{B})}{\mathbb{P}(A + xR_1 + \lambda \in \mathcal{B})} \leq e^{\bar{\epsilon}} \leq e^{\epsilon}. \tag{62}$$

Without loss of generality, we assume that the first T nodes collude, i.e., $\mathcal{T} = \{1, 2, ..., \mathsf{T}\}$. Under this setting, T colluders collect:

$$\begin{aligned}
\mathbf{Z} &= (A + xR_1)\mathbf{1} + \begin{bmatrix} h_1 & h_2 & \cdots & h_{\mathsf{T}} \end{bmatrix}^T \alpha_1^{(n)} R_1 + \alpha_2^{(n)} \begin{bmatrix} \mathbf{g_1} & \mathbf{g_2} & \cdots & \mathbf{g}_{\mathsf{T}} \end{bmatrix}^T \begin{bmatrix} R_2 & R_3 & \cdots & R_{\mathsf{T}} \end{bmatrix}^T \\
&= (A + xR_1)\mathbf{1} + \bar{\mathbf{G}} \begin{bmatrix} \alpha_1^{(n)} R_1 & \alpha_2^{(n)} R_2 & \cdots & \alpha_2^{(n)} R_{\mathsf{T}} \end{bmatrix}^T,
\end{aligned} \tag{63}$$

where $\bar{\mathbf{G}} = \begin{bmatrix} h_1 & h_2 & \cdots & h_{\mathsf{T}} \\ \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_{\mathsf{T}} \end{bmatrix}^T$ As the matrix $\bar{\mathbf{G}}$ is full-rank according to the designed scheme, colluders can map $\mathbf{Z}$ to

$$(A + xR_1)\bar{\mathbf{G}}^{-1}\mathbf{1} + \begin{bmatrix} \alpha_1^{(n)} R_1 & \alpha_2^{(n)} R_2 & \cdots & \alpha_2^{(n)} R_{\mathsf{T}} \end{bmatrix}^T. \tag{64}$$

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 first prove 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 $\mathbf{g'}_1^T \begin{bmatrix} \mathbf{g_1} & \mathbf{g_2} & \cdots & \mathbf{g}_{\mathsf{T}} \end{bmatrix}^T = \mathbf{0}^T$, it follows that $\mathbf{g'}_i^T \mathbf{1}$ cannot be zero.

We can then normalize the first component of the mapped $\mathbf{Z}$ and obtain $A + xR_1 + \frac{1}{\mathbf{g'}_1^T \mathbf{1}} \alpha_1^{(n)} R_1$. Next, we can use the term $A + xR_1 + \frac{1}{\mathbf{g'}_1^T \mathbf{1}} \alpha_1^{(n)} R_1$ to cancel out the R_1 term in the other component of $\mathbf{Z}$. Therefore based on the original $\mathbf{Z}$ there exists a full-rank matrix $\mathbf{V}$ of size $\mathsf{T} \times \mathsf{T}$ such that $\mathbf{Z}' = \mathbf{V}\mathbf{Z}$, where [3]

$$\mathbf{Z}' = \begin{bmatrix} A + xR_1 + \frac{1}{\mathbf{g'}_1^T \mathbf{1}} \alpha_1^{(n)} R_1 & A + \frac{\alpha_2^{(n)} \left(\alpha_1^{(n)} + \mathbf{g'}_1^T \mathbf{1} x\right)}{\alpha_1^{(n)} \mathbf{g'}_2^T \mathbf{1}} R_2 & \cdots & A + \frac{\alpha_2^{(n)} \left(\alpha_1^{(n)} + \mathbf{g'}_1^T \mathbf{1} x\right)}{\alpha_1^{(n)} \mathbf{g'}_{\mathsf{T}}^T \mathbf{1}} R_{\mathsf{T}} \end{bmatrix}^T \tag{65}$$

[3]Note that we only consider the non-trivial case where $\mathbf{g'}_i^T \mathbf{1} \neq 0$. When $\mathbf{g'}_i^T \mathbf{1} = 0$, the privacy is well-preserved as there is only noise remaining.

We denote $\mathbf{Z}' = \begin{bmatrix} Z_1' & Z_2' & \cdots & Z_{\mathsf{T}}' \end{bmatrix}^T$, and each Z_i' with $i \in [\mathsf{T}]$ can be viewed as the linear combination of A and R_i. Based on the post-processing property of DP [7] (performing arbitrary computations on the output of a differentially private mechanism would not increase the privacy loss), $\mathbf{Z}' = \mathbf{1}\mathbf{Z}$ satisfies the DP guarantee of $\mathbf{Z}$, where $\mathbf{1}$ denotes a linear transformation matrix of size $\mathsf{T} \times \mathsf{T}$, i.e., $\mathbf{Z}'$ remains differentially private with at least the same level of privacy as $\mathbf{Z}$.

For $2 \leq i \leq \mathsf{T}$,the i-th term of Z_i' is $A + \frac{\alpha_2^{(n)}\left(\alpha_1^{(n)} + \mathbf{g'}_1^T \mathbf{1} x\right)}{\alpha_1^{(n)} \mathbf{g'}_i^T \mathbf{1}} R_i$, where the second term is a Laplace random variable with variance $\left(\frac{\alpha_2^{(n)}\left(\alpha_1^{(n)} + \mathbf{g'}_1^T \mathbf{1} x\right)}{\alpha_1^{(n)} \mathbf{g'}_i^T \mathbf{1}}\right)^2$. As the added Laplace random noise with distribution Lap($\frac{1}{\epsilon}$) brings ϵ-DP [8], Z_i' is a privacy mechanism that achieves $\frac{\alpha_1^{(n)} \mathbf{g'}_i^T \mathbf{1}}{\alpha_2^{(n)}\left(\alpha_1^{(n)} + \mathbf{g'}_1^T \mathbf{1} x\right)} \sqrt{2}$-DP as $R_2, R_3, \cdots, R_{\mathsf{T}}$ are independent unit variance Laplace random variables.

For $i = 1$, we have that

$$\begin{aligned} &\sup_{\mathcal{B} \in \mathbb{R}, -1 < \lambda < 1} \frac{\mathbb{P}(A + (x + \frac{1}{\mathbf{g'}_1^T \mathbf{1}} \alpha_1^{(n)}) R_1 \in \mathcal{B})}{\mathbb{P}(A + (x + \frac{1}{\mathbf{g'}_1^T \mathbf{1}} \alpha_1^{(n)}) R_1 + \lambda \in \mathcal{B})} \\ =& \sup_{\mathcal{B} \in \mathbb{R}, -\frac{x}{x + \frac{1}{\mathbf{g'}_1^T \mathbf{1}} \alpha_1^{(n)}} < \lambda < \frac{x}{x + \frac{1}{\mathbf{g'}_1^T \mathbf{1}} \alpha_1^{(n)}}} \frac{\mathbb{P}(A + x R_1 \in \mathcal{B})}{\mathbb{P}(A + x R_1 + \lambda \in \mathcal{B})} \\ \overset{(a)}{\leq}& e^{\bar{\epsilon}} + \delta' \leq e^{\epsilon}, \end{aligned} \tag{66}$$

where (a) holds as $\lim_{n \to \infty} \frac{x}{x + \frac{1}{\mathbf{g'}_1^T \mathbf{1}} \alpha_1^{(n)}} = 1$ and for any $\delta' > 0$. Hence Z_1' achieves ϵ-DP.

Since $R_1, R_2, ..., R_{\mathsf{T}}$ are independent, $\mathbf{Z}'$ achieves $\epsilon + \sqrt{2} \sum_{i=2}^{\mathsf{T}} \frac{\alpha_1^{(n)} \mathbf{g'}_1^T \mathbf{1}}{\alpha_2^{(n)}\left(\alpha_1^{(n)} + \mathbf{g'}_1^T \mathbf{1} x\right)}$-DP due to the composition theorem [7]. As $\lim_{n \to \infty} \frac{\alpha_1^{(n)}}{\alpha_2^{(n)}} = 0$, the DP parameter tends to be ϵ as $n \to \infty$. Hence we have proved the proposed scheme satisfies T-node ϵ-DP.

VI. Numerical Stability Analysis

Note that the proposed coding scheme operates in the real domain, where real numbers cannot be directly represented with the given finite number of bits, resulting in an inherent loss of accuracy. For an unstable linear system, a small perturbation of the input may lead to a large error of the output. The condition number κ measures the sensitivity of the system, and a large condition number for a linear system indicates that the system is ill-conditioned, where the output is highly sensitive to small changes in the input. Considering a linear system $\mathbf{A}\mathbf{x} = \mathbf{b}$, where $\mathbf{A}$ is a non-singular square matrix and $\mathbf{x}, \mathbf{b}$ are some column vectors, the matrix condition number of $\mathbf{A}$ is defined as $\kappa(\mathbf{A}) = \|\mathbf{A}\| \|\mathbf{A}^{-1}\|$.

For the proposed coding method proposed in Section III, the encoding process can be viewed as the multiplication of the encoding matrix $\mathbf{M}$ with the vector $\begin{bmatrix} A + xR_1 & \alpha_2^{(n)} R_2 & \cdots & \alpha_2^{(n)} R_{\mathsf{T}} & \alpha_1^{(n)} R_1 \end{bmatrix}^T$. By ignoring terms of magnitude $O\left((\alpha_2^{(n)})^2\right)$ (as we do in the decoding process in Section III), the computation results can be interpreted as the multiplication of matrix $\mathbf{M}$ with the message vector $\{m_i\}_{i=1}^{\mathsf{T}+1}$ as shown in (51). The decoding process involves multiplying the received messages (after removing the detected error results) by a $(\mathsf{T}+1) \times (\mathsf{T}+1)$ submatrix and $\mathsf{T} \times \mathsf{T}$ submatrix matrix of the encoding matrix $\mathbf{M}$, respectively, and then obtain the estimated result. Hence,

to ensure the numerical stability of the coding scheme, we aim to ensure that the condition number κ of every $(\mathsf{T}+1)\times(\mathsf{T}+1)$ submatrix of the $\mathsf{N}\times(\mathsf{T}+1)$ matrix $\mathbf{M}$ grows slowly with the dimensional N by selecting a proper polynomial basis set $\{1, f_1, f_2, \cdots, f_{\mathsf{T}}\}$. Here we present two choices and analyze their condition number properties.

1) Monomial polynomials: A common approach in the coding computation literature is to use monomial polynomials polynomials $\{1, x, x^2, \cdots, x^{\mathsf{T}}\}$ [9]. In this case, the encoding matrix can be written as follows.

$$\mathbf{M} = \begin{bmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{\mathsf{T}} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{\mathsf{T}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_{\mathsf{N}} & a_{\mathsf{N}}^2 & \cdots & a_{\mathsf{N}}^{\mathsf{T}} \end{bmatrix}_{\mathsf{N}\times(\mathsf{T}+1)}, \tag{67}$$

with N distinct non-zero evaluation points $\{a_i\}_{i=1}^{\mathsf{N}}$. However, the monomial polynomials empirically demonstrate poor scalability since the condition number of the Vandermonde matrix grows exponentially with the dimension N [10], [11], [12]. Loss of precision due to digital storage can cause significant output errors [13].

2) Chebyshev polynomials: To remedy the numerical instability of the Vandermonde matrix, [12] utilizes Chebyshev polynomials instead of monomial polynomials to construct polynomial-based codes. The Chebyshev polynomials of the first kind [14] are obtained from the recurrence relation as follows.

$$T_i = 2aT_{i-1} - T_{i-2}, \quad \text{for} \quad i > 2, \tag{68}$$

and $T_0 = 1$, $T_1 = a$. We let $\{\rho_i^{(\mathsf{N})}\}_{i=1}^{\mathsf{N}}$ denote Chebyshev nodes, which are roots or extrema of the Chebyshev T_{N}, given by $\rho_i^{(\mathsf{N})} = \cos\left(\frac{(2i-1)\pi}{2\mathsf{N}}\right)$ for $i \in [\mathsf{N}]$. Selecting $\{T_0, T_1, \cdots, T_{\mathsf{T}}\}$ as the encoding polynomials of the coding scheme and utilizing $\{\rho_i^{(\mathsf{N})}\}_{i=1}^{\mathsf{N}}$ as the evaluation points, the encoding matrix $\mathbf{M}$ with $\mathsf{N} > \mathsf{T}$ can be written as follows.

$$\mathbf{M} = \begin{bmatrix} 1 & T_1(\rho_1^{(\mathsf{N})}) & T_2(\rho_1^{(\mathsf{N})}) & \cdots & T_{\mathsf{T}}(\rho_1^{(\mathsf{N})}) \\ 1 & T_1(\rho_2^{(\mathsf{N})}) & T_2(\rho_2^{(\mathsf{N})}) & \cdots & T_{\mathsf{T}}(\rho_2^{(\mathsf{N})}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & T_1(\rho_{\mathsf{N}}^{(\mathsf{N})}) & T_2(\rho_{\mathsf{N}}^{(\mathsf{N})}) & \cdots & T_{\mathsf{T}}(\rho_{\mathsf{N}}^{(\mathsf{N})}) \end{bmatrix}_{\mathsf{N}\times(\mathsf{T}+1)}, \tag{69}$$

Note that [12] shows that the condition number of every $(\mathsf{T}+1)\times(\mathsf{T}+1)$ submatrix of the above encoding matrix grows as $O(\mathsf{N}^{2(\mathsf{N}-\mathsf{T}-1)})$, which significantly improves numerical stability compared to the Vandermonde matrix.

VII. Conclusion

In this paper, we proposed a novel coding scheme that achieves T-node ϵ-DP, E-node resiliency, and A-node security.

References

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

[2] 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.

[3] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation," in *Providing sound foundations for cryptography: on the work of Shafi Goldwasser and Silvio Micali*, 2019, pp. 351–371.

[4] 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.

[5] 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.

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

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

[8] 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.

[9] 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.

[10] W. Gautschi and G. Inglese, "Lower bounds for the condition number of vandermonde matrices," *Numerische Mathematik*, vol. 52, no. 3, pp. 241–250, 1987.

[11] W. Gautschi, "How (un) stable are vandermonde systems?" in *Asymptotic and computational analysis*. CRC Press, 2020, pp. 193–210.

[12] M. Fahim and V. R. Cadambe, "Numerically stable polynomially coded computing," *IEEE Transactions on Information Theory*, vol. 67, no. 5, pp. 2758–2785, 2021.

[13] U. Sheth, S. Dutta, M. Chaudhari, H. Jeong, Y. Yang, J. Kohonen, T. Roos, and P. Grover, "An application of storage-optimal matdot codes for coded matrix multiplication: Fast k-nearest neighbors estimation," in *2018 IEEE International Conference on Big Data (Big Data)*. IEEE, 2018, pp. 1113–1120.

[14] L. N. Trefethen, *Approximation theory and approximation practice, extended edition*. SIAM, 2019.