Implementation of $\mathsf{SecCos}(\llbracket g_a \rrbracket, \llbracket g_b \rrbracket)$

Given two encrypted gradients $\llbracket g_a \rrbracket = \{\llbracket x'_{a_1} \rrbracket, \llbracket x'_{a_2} \rrbracket, ..., \llbracket x'_{a_m} \rrbracket\}$ and $\llbracket g_b \rrbracket = \{\llbracket x'_{b_1} \rrbracket, \llbracket x'_{b_2} \rrbracket, ..., \llbracket x'_{b_m} \rrbracket\}$:

- @$\mathcal{S}_1$: Once receiving $\llbracket g_a \rrbracket$ and $\llbracket g_b \rrbracket$, $\mathcal{S}_1$ first selects m random noises $r_{k\in[1,m]} \leftarrow \mathbb{Z}_N^*$, and blinds r_k to $\llbracket g_a \rrbracket$ and $\llbracket g_b \rrbracket$. As computed in Eq. 14, $\llbracket \overline{g}_a \rrbracket = \{\llbracket \overline{x}_{a_1} \rrbracket, ..., \llbracket \overline{x}_{a_m} \rrbracket\}$ and $\llbracket \overline{g}_b \rrbracket = \{\llbracket \overline{x}_{b_1} \rrbracket, ..., \llbracket \overline{x}_{b_m} \rrbracket\}$ are obtained. Then, $\mathcal{S}_1$ executes

$$[\overline{x}_{a_k}]_1 \leftarrow \mathsf{PartDec}_{sk_1}(\llbracket \overline{x}_{a_k} \rrbracket),\ [\overline{x}_{b_k}]_1 \leftarrow \mathsf{PartDec}_{sk_1}(\llbracket \overline{x}_{b_k} \rrbracket),$$
$$s.t.,\ \llbracket \overline{x}_{a_k} \rrbracket \in \llbracket \overline{g}_a \rrbracket, \llbracket \overline{x}_{b_k} \rrbracket \in \llbracket \overline{g}_b \rrbracket,$$

  and sends $[\overline{g}_a]_1, [\overline{g}_b]_1, \llbracket \overline{g}_a \rrbracket, \llbracket \overline{g}_b \rrbracket$ to $\mathcal{S}_2$.
- @$\mathcal{S}_2$: Once obtaining these encrypted numbers, $\mathcal{S}_2$ calls $\mathsf{PartDec}$ and $\mathsf{FullDec}$ to obtain $\overline{g_a}$ and $\overline{g_b}$. Then, $\mathcal{S}_2$ implements

$$\overline{\cos}_{ab} = \overline{g_a} \odot \overline{g_b} = \Sigma_{k=1}^{m} \overline{x}_{a_k} \cdot \overline{x}_{b_k}. \tag{16}$$

  $\mathcal{S}_2$ calls the Enc algorithm to return $\llbracket \overline{\cos}_{ab} \rrbracket$ to $\mathcal{S}_1$.
- @$\mathcal{S}_1$: To remove the noise r_k in $\llbracket \overline{\cos}_{ab} \rrbracket$, $\mathcal{S}_1$ implements Eq. 15 to obtain the final cosine similarity $\llbracket \cos_{ab} \rrbracket$.
- @$\mathcal{S}_2$: The decryption share $[\cos_{ab}]_2 \leftarrow \mathsf{PartDec}_{sk_2}(\llbracket \cos_{ab} \rrbracket)$ is executed to return $\mathcal{S}_1$.
- @$\mathcal{S}_1$: To obtain $\cos_{ab}$ between $\llbracket g_a \rrbracket$ and $\llbracket g_b \rrbracket$ as shown in Eq. 13, $\mathcal{S}_1$ computes the cosine similarity $\cos_{ab}$ with $[\cos_{ab}]_2 \leftarrow \mathsf{PartDec}_{sk_2}(\llbracket \cos_{ab} \rrbracket)$ and $\cos_{ab} \leftarrow \mathsf{FullDec}([\cos_{ab}]_1, [\cos_{ab}]_2)$. Note that the precise degree of $\cos_{ab}$ is expanded as deg^2 after $\mathsf{HE.Mul}$. To keep the degree deg consistent, the final result is truncated as $\cos_{ab} \leftarrow \lfloor \frac{\cos_{ab}}{deg} \rceil$.