

| Notations                 | Descriptions                  | Notations      | Descriptions                  |
|---------------------------|-------------------------------|----------------|-------------------------------|
| $\mathbb{Z}_{N^2}^*$      | Ciphertext space              | $\mathbb{Z}_N$ | Plaintext space               |
| $pk, sk$                  | Public/secret key             | $sk_i$         | Secret key share              |
| $\llbracket x \rrbracket$ | Ciphertext                    | $[x]_i$        | Decryption share with $sk_i$  |
| $g_i$                     | Local gradient                | $g$            | Aggregated gradient           |
| $g_i^*$                   | Poisonous gradient            | $W^*$          | Poisoned model                |
| $W_i^{(t)}$               | Local model                   | $W^{(t)}$      | Global model                  |
| Appr                      | Approximation function        | $deg$          | Precision degree              |
| HE.Mul                    | Secure multiplication         | SecJudge       | Normalization judgment        |
| SecCos                    | Secure cosine similarity      | cos            | cosine similarity value       |
| $Acc$                     | Overall accuracy              | $Acc_{source}$ | Source accuracy               |
| $AI$                      | Improvement of $Acc$          | $ASR$          | Attack success rate           |
| $AI_{source}$             | Improvement of $Acc_{source}$ | $\eta_i$       | Confidence of $\mathcal{U}_i$ |