Algorithm 3 Privacy-Preserving Defense Strategy

Input: The local gradients $\{[\![g_1^{(t)}]\!], \ldots, [\![g_n^{(t)}]\!]\}$.
Output: Aggregated gradients $[\![g^{(t)}]\!]$.

if $t == 1$ **then**
  $[\![g^{(t)}]\!] \leftarrow [\![g_1^{(t)}]\!] \cdot [\![g_2^{(t)}]\!] \cdot \ldots \cdot [\![g_n^{(t)}]\!]$;
  $[\![g^{(t)}]\!] \leftarrow \mathsf{HE.Trun}([\![g^{(t)}]\!], n)$;
for $i \in [1, n]$ **do**
  */*Normalization judgment*/*
  $sum \leftarrow \mathsf{SecJudge}([\![g_i^{(t)}]\!])$;
  if $sum/deg^2 == 1$ **then**
    */*Secure cosine similarity*/*
    $\cos_i \leftarrow \mathsf{SecCos}([\![g_i^{(t)}]\!], [\![g^{(t-1)}]\!])$;
Find the gradient $[\![g^*]\!]$ with the lowest cosine similarity cos as the baseline of poisonous gradients;
*/*Byzantine-tolerance aggregation*/*
$[\![g^{(t)}]\!] \leftarrow [\![0]\!]$;
for $i \in [1, n]$ **do**
  $\cos_i \leftarrow \mathsf{SecCos}([\![g_i^{(t)}]\!], [\![g^*]\!])$;
  $\eta_i \leftarrow deg - \cos_i$;
for $i \in [1, n]$ **do**
  $\eta_i \leftarrow \lceil \frac{\eta_i}{\sum_{i=1}^{n} \eta_i} \cdot deg \rfloor$;
  $[\![g^{(t)}]\!] \leftarrow [\![g^{(t)}]\!] \cdot [\![g_i^{(t)}]\!]^{\eta_i}$ based on Eq. 5;
return The aggregated gradient $[\![g^{(t)}]\!]$.