We sincerely appreciate your valuable suggestions. Herein, we provide the notation table from the original text, which will also be included in the revised paper:

Notation	Description
N	The node counts in the graph
M	The slot counts in a ciphertext
F	Feature counts of a certain layer's input
$F^{'}$	Feature counts of a certain layer's output
n	The sampled neighbor counts
t	The number of node features simultaneously packed into a single ciphertext

The upper bound of rotations in SpIntra-CA is $log^2(N)$ rather than $O(N)$ because the aggregation process has the "conflict-free to conflict-free" restriction. This can be formally proved by the correctness of Lemma 1 and Conflict Upper Bound Analysis.

Consider the worst-case situation where $Con(j) = 2^j$, the rotation step (rs) bits at each stage are uniformly distributed across all elements. However, this would lead to all elements being concentrated in a single slot in the final aggregation result. Consequently, to ensure a conflict-free final output, there is a loose constraint on the maximum allowable conflicts at each stage: $Con(j) \leq min\{2^j, 2^{log(N)-1-j}\},\ j = 0, 1, ..., log(N) - 1$. This remains a loose constraint because it can be resolved through trivial stage ordering adjustment, which is part of our algorithm. Below we provide a rigorous proof establishing the tight upper bound ($O(log^2 N)$) for the number of rotations.

Analysis: 1) $Con_{i,j}$, denoting the number of conflicts in the i^{th} rotation stage at the j^{th} slot, can be written as the summation of all conflicts during the prior stages in the corresponding slots which can be rotated to j^{th}. 2) $PR(ct[m] \rightarrow ct[q])$, denotes the the probability of an element in m^{th} slot rotated to q^{th} under SpIntra-CA. The case "$ct[j + \sum_{p=0}^{k-1} 2^p] \rightarrow ct[j]$" means that the rotation step(rs) bits of an element in $ct[j + \sum_{p=0}^{k-1} 2^p]$ should be all "1" among the corresponding k contiguous bits. For example , without loss of generality, considering the first 3 stages, the elements in j^{th} slot is rotated directly from $(j+7)^{th}, (j+3)^{th}, (j+1)^{th}$ slots, indicating elements in the corresponding slots have the 3,2,1 contiguous "1" LSB.

Lemma 1: Given any bit distribution($Pr[bit_p = 1] = \frac{1}{2} - \epsilon,\ \epsilon \in [-\frac{1}{2}, \frac{1}{2}]$), $PR(ct[j + \sum_{p=0}^{k-1} 2^p] \rightarrow ct[j]) \leq \frac{1}{2^k}$

Proof: Based on *Analysis* 2), we have

$$PR(ct[j + \sum_{p=0}^{k-1} 2^p] \rightarrow ct[j]) = (\frac{1}{2} - \epsilon)^k$$

. So lemma 1 holds trivially when $\epsilon > 0$. When $\epsilon \leq 0$, by replacing cyclic left

shifts with cyclic right shifts, the rs bits become the complement of the original:

$$PR(ct[j + \sum_{p=0}^{k-1} 2^p] \rightarrow ct[j]) = (\frac{1}{2} + \epsilon)^k \leq \frac{1}{2^k}$$

. So we have $PR(ct[j + \sum_{p=0}^{k-1} 2^p] \rightarrow ct[j]) < \frac{1}{2^k}$ when $\epsilon \neq 0$.Consequently, the worst-case scenario occurs when all rs bits are independently and uniformly distributed.

Conflict Upper Bound Analysis: $Con_{i,j} \leq log(N)$ under the worst case(uniform distribution).

Proof: According to *Analysis* 1),

$$Con_{i,j} = \sum_{k=0}^{i-1} Con_{k,j+\sum_{p=0}^{k-1} 2^p} \cdot PR(ct[j + \sum_{p=0}^{k-1} 2^p] \rightarrow ct[j])$$

According to Lemma 1, it is

$$\sum_{k=0}^{i-1} Con_{k,j+\sum_{p=0}^{k-1} 2^p} \cdot \frac{1}{2^k} \leq \sum_{k=0}^{i-1} 2^k \cdot \frac{1}{2^k} = i \leq log(N)$$

Thus, the number of conflicts per stage is bounded by log(N), yielding a total conflict complexity of less than $log^2(N)$ between an aggregation of two nodes.

While the above analysis proves our algorithm has a theoretically low upper bound for rotation overhead, the worst-case scenario rarely occurs in practice, thereby yielding significantly more efficient computation. To validate this, we conducted multiple randomized reordering experiments with varying N to simulate diverse scenarios during aggregation. We conduct different random permutations 10000 times for each case, and the results including the maximum number of rotation(Max), the average rotation counts(Avg) and the standard deviation(SD) are presented in the following table:

N	Max	Avg	SD	Worst Case
2^{12}	96	84	4.60	144
2^{13}	102	87	6.71	169
2^{14}	110	97	6.55	196