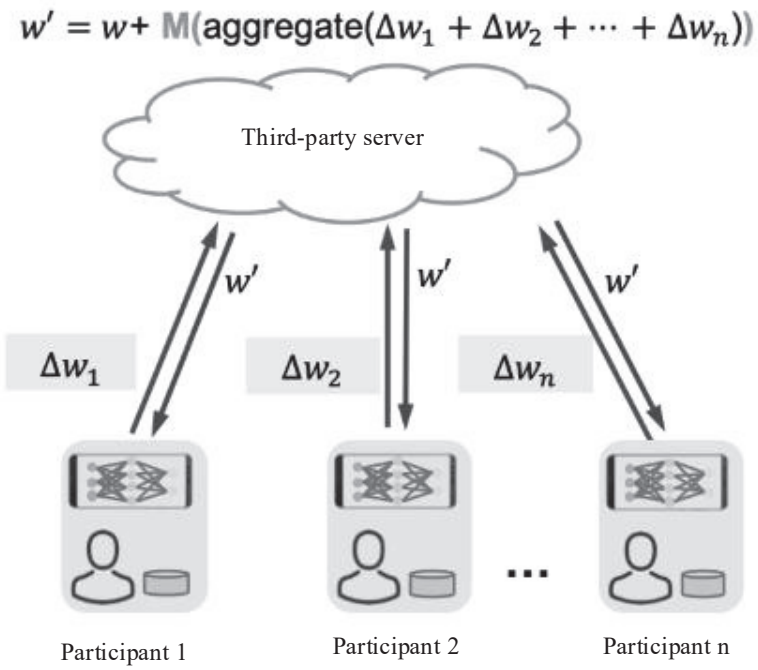

$w' = w + M(\text{aggregate}(\Delta w_1 + \Delta w_2 + \cdots + \Delta w_n))$
Third-party server
w'
w'
w'
Δw_1
Δw_2
Δw_n
Participant 1
Participant 2
Participant n

FIG. 1

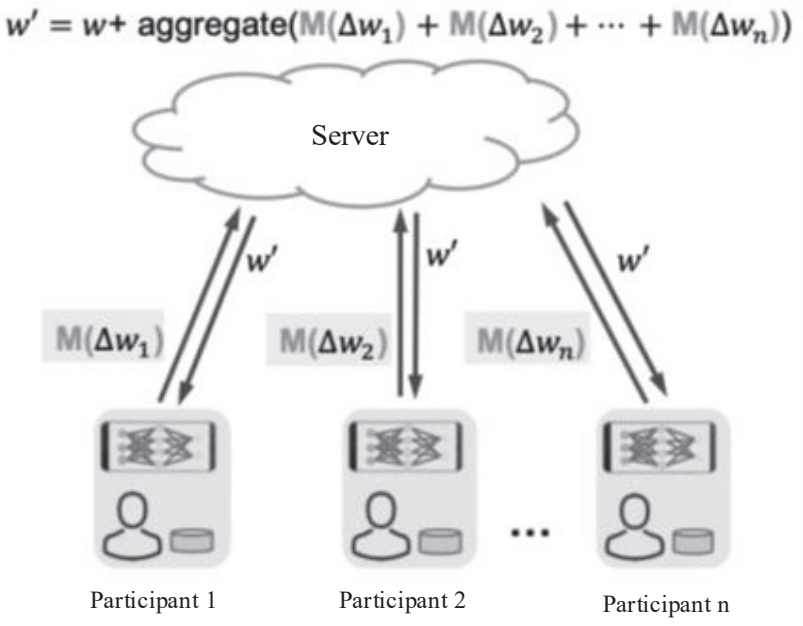

$w' = w + \text{aggregate}(M(\Delta w_1) + M(\Delta w_2) + \cdots + M(\Delta w_n))$
Server
w'
w'
w'
$M(\Delta w_1)$
$M(\Delta w_2)$
$M(\Delta w_n)$
Participant 1
Participant 2
Participant n

FIG. 2

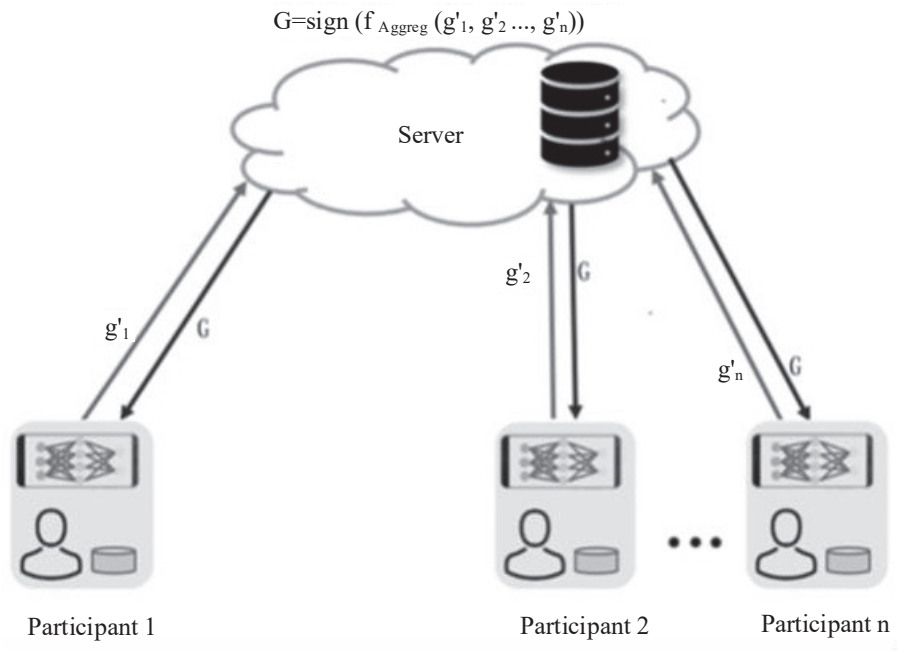

G=sign (f Aggreg (g'1, g'2 ..., g'n))
Server
g'1
G
g'2
G
g'n
G
Participant 1
Participant 2
Participant n

FIG. 3

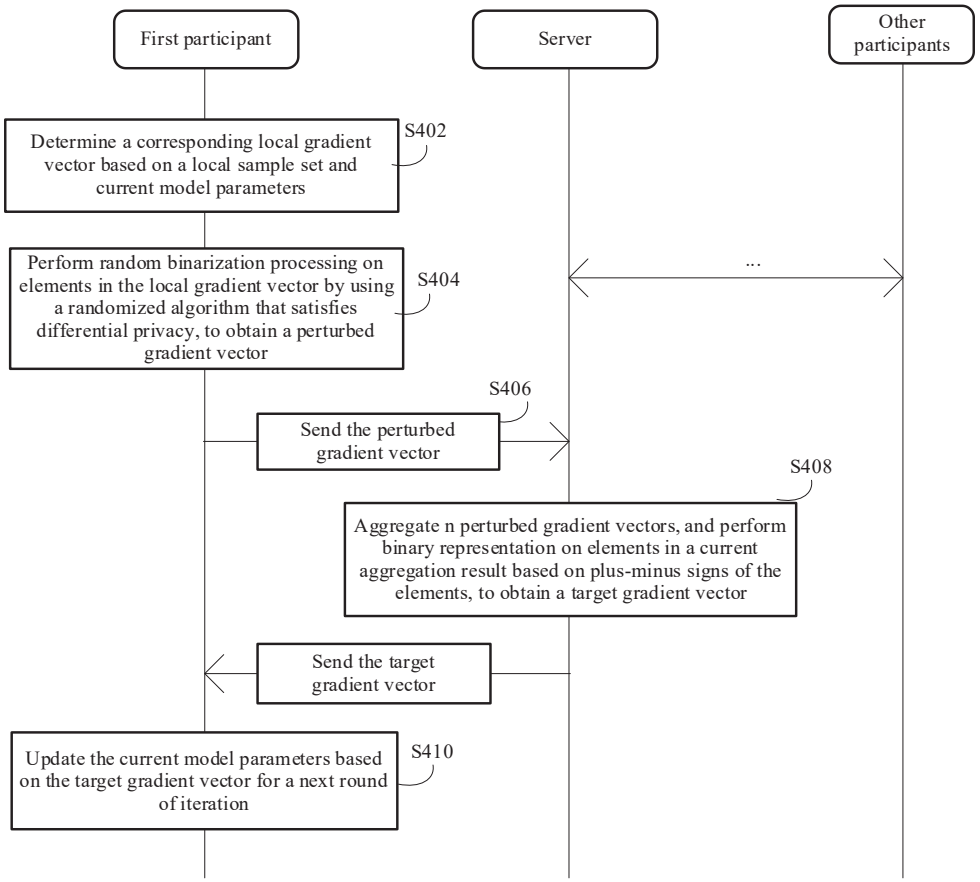

First participant
Server
Other participants
Determine a corresponding local gradient vector based on a local sample set and current model parameters
S402
Perform random binarization processing on elements in the local gradient vector by using a randomized algorithm that satisfies differential privacy, to obtain a perturbed gradient vector
S404
...
S406
Send the perturbed gradient vector
S408
Aggregate n perturbed gradient vectors, and perform binary representation on elements in a current aggregation result based on plus-minus signs of the elements, to obtain a target gradient vector
Send the target gradient vector
Update the current model parameters based on the target gradient vector for a next round of iteration
S410

FIG. 4

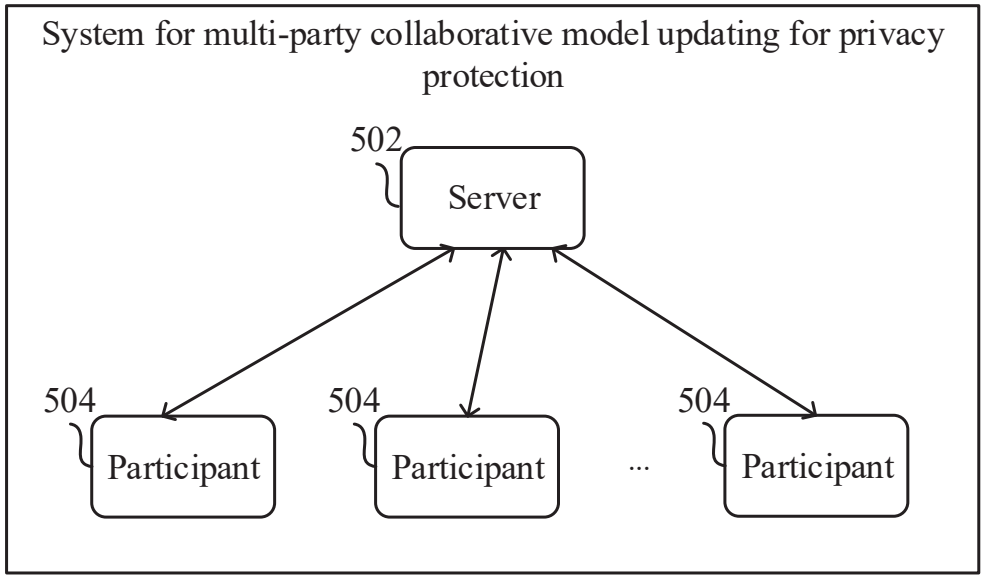

System for multi-party collaborative model updating for privacy protection
502
Server
504
Participant
504
Participant
...
504
Participant

FIG. 5

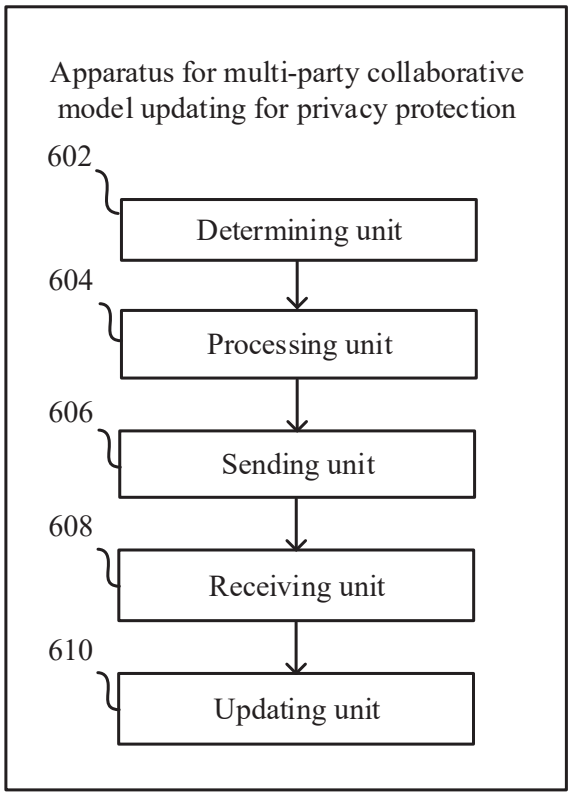

Apparatus for multi-party collaborative model updating for privacy protection
602
Determining unit
604
Processing unit
606
Sending unit
608
Receiving unit
610
Updating unit

FIG. 6