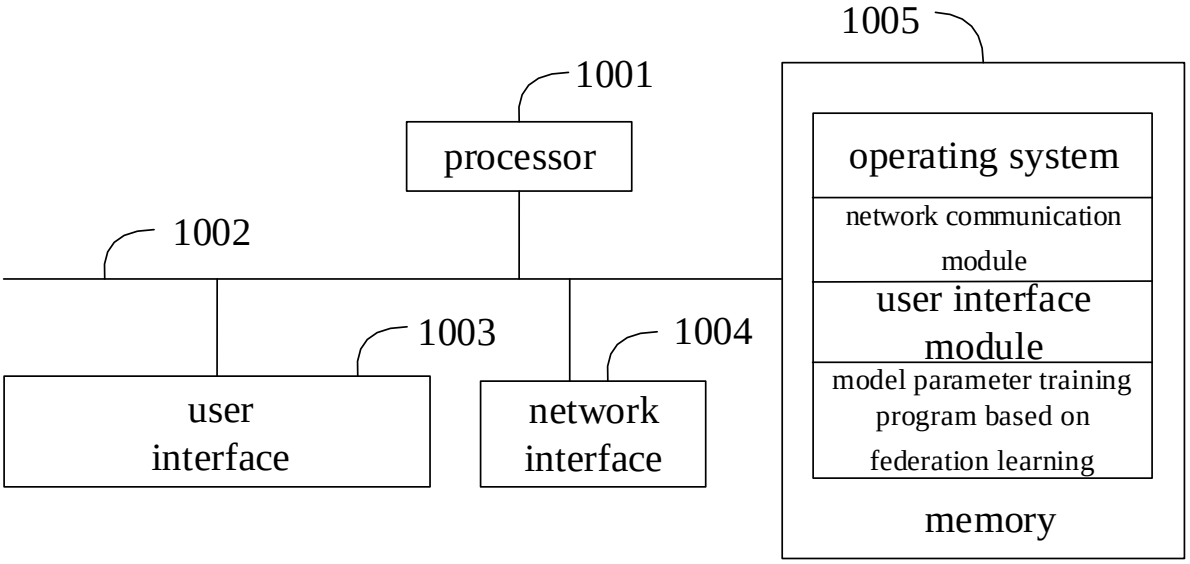
1005
1001
processor
operating system
network communication module
1002
user interface module
1003
1004
user interface
network interface
model parameter training program based on federation learning
memory

FIG. 1

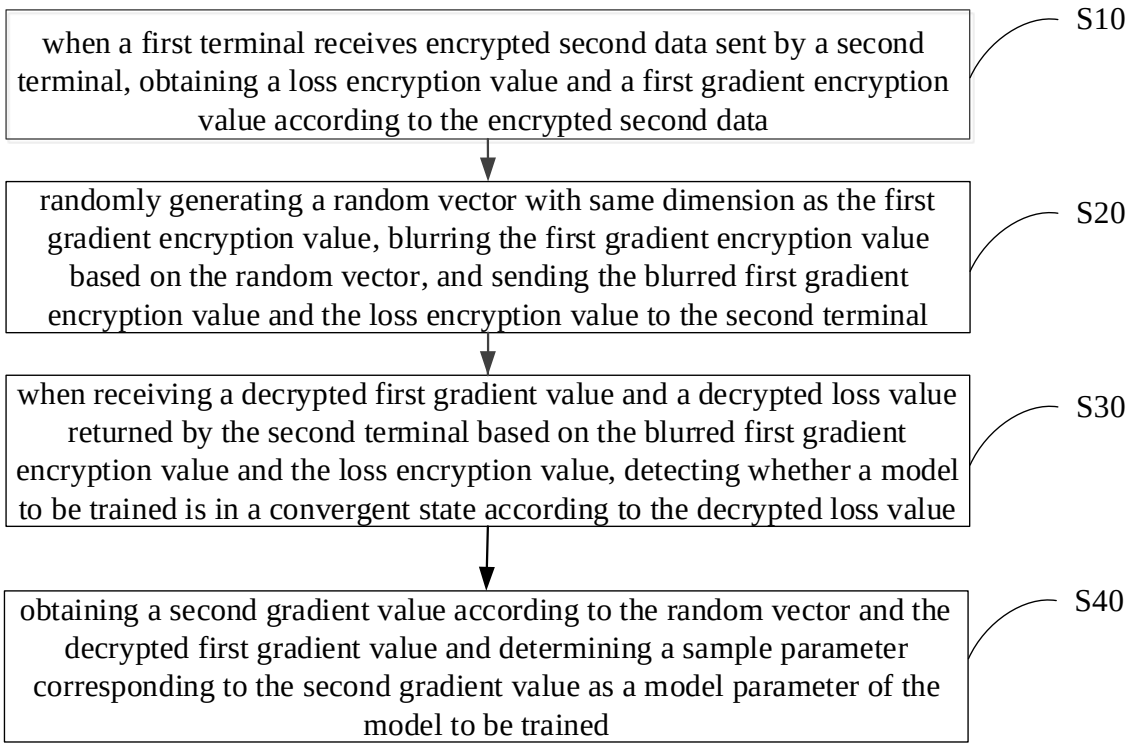
when a first terminal receives encrypted second data sent by a second terminal, obtaining a loss encryption value and a first gradient encryption value according to the encrypted second data
S10
randomly generating a random vector with same dimension as the first gradient encryption value, blurring the first gradient encryption value based on the random vector, and sending the blurred first gradient encryption value and the loss encryption value to the second terminal
S20
when receiving a decrypted first gradient value and a decrypted loss value returned by the second terminal based on the blurred first gradient encryption value and the loss encryption value, detecting whether a model to be trained is in a convergent state according to the decrypted loss value
S30
obtaining a second gradient value according to the random vector and the decrypted first gradient value and determining a sample parameter corresponding to the second gradient value as a model parameter of the model to be trained
S40

FIG. 2

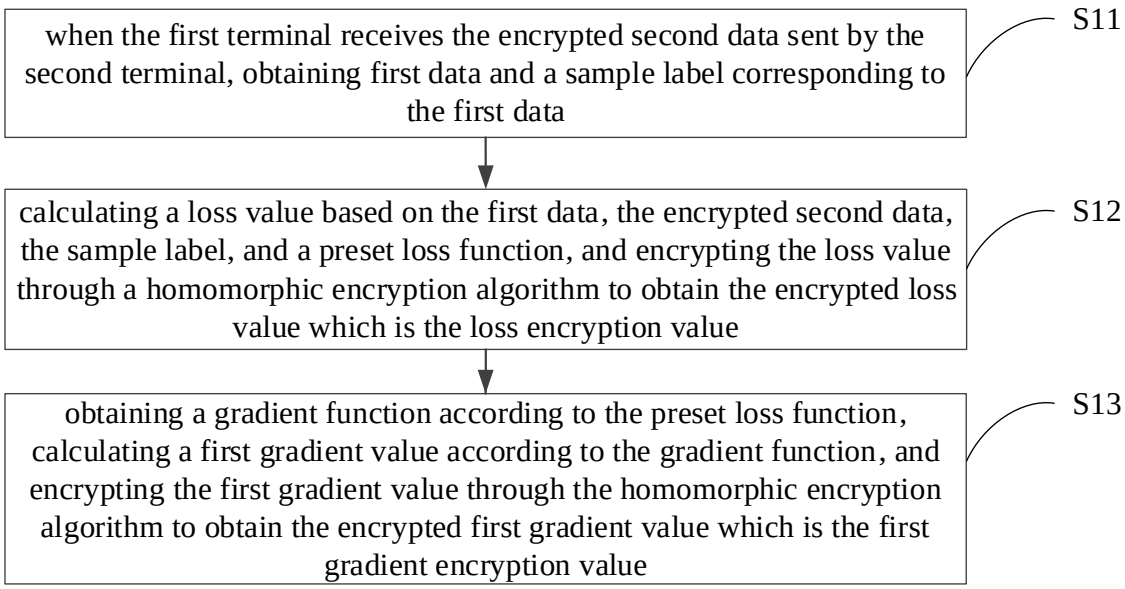
when the first terminal receives the encrypted second data sent by the second terminal, obtaining first data and a sample label corresponding to the first data
S11
calculating a loss value based on the first data, the encrypted second data, the sample label, and a preset loss function, and encrypting the loss value through a homomorphic encryption algorithm to obtain the encrypted loss value which is the loss encryption value
S12
obtaining a gradient function according to the preset loss function, calculating a first gradient value according to the gradient function, and encrypting the first gradient value through the homomorphic encryption algorithm to obtain the encrypted first gradient value which is the first gradient encryption value
S13

FIG. 3

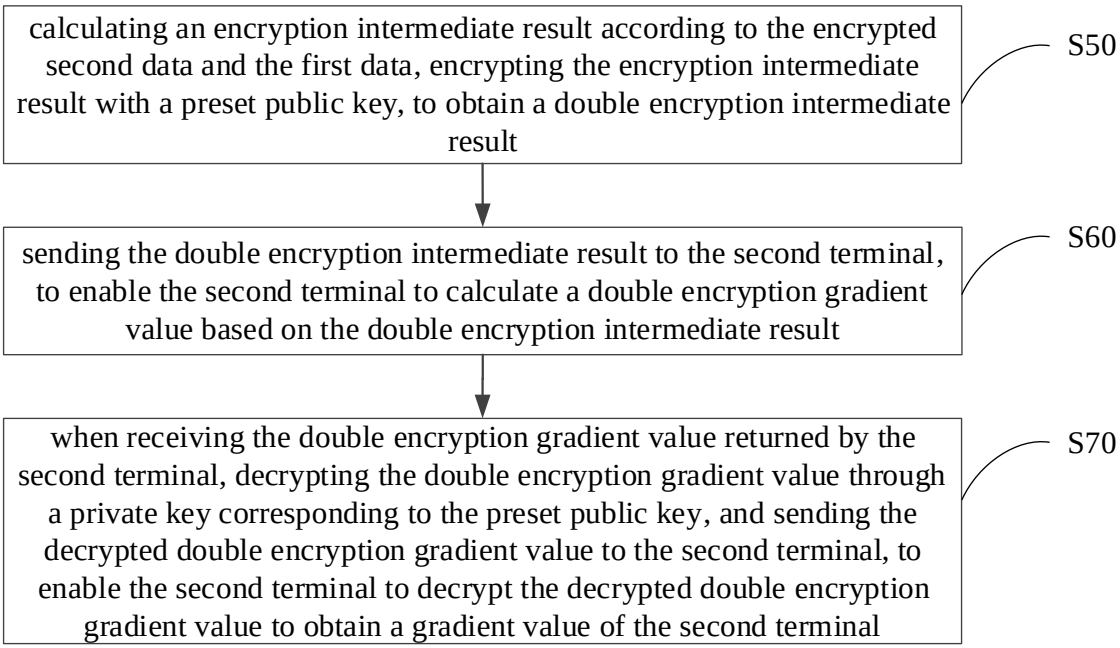
calculating an encryption intermediate result according to the encrypted second data and the first data, encrypting the encryption intermediate result with a preset public key, to obtain a double encryption intermediate result
S50
sending the double encryption intermediate result to the second terminal, to enable the second terminal to calculate a double encryption gradient value based on the double encryption intermediate result
S60
when receiving the double encryption gradient value returned by the second terminal, decrypting the double encryption gradient value through a private key corresponding to the preset public key, and sending the decrypted double encryption gradient value to the second terminal, to enable the second terminal to decrypt the decrypted double encryption gradient value to obtain a gradient value of the second terminal
S70

FIG. 4

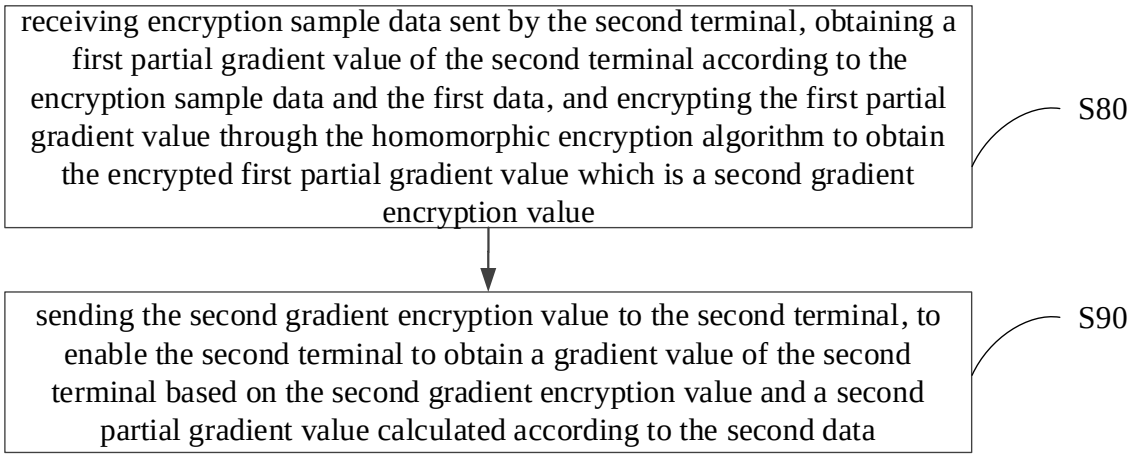
receiving encryption sample data sent by the second terminal, obtaining a first partial gradient value of the second terminal according to the encryption sample data and the first data, and encrypting the first partial gradient value through the homomorphic encryption algorithm to obtain the encrypted first partial gradient value which is a second gradient encryption value
S80
sending the second gradient encryption value to the second terminal, to enable the second terminal to obtain a gradient value of the second terminal based on the second gradient encryption value and a second partial gradient value calculated according to the second data
S90

FIG. 5

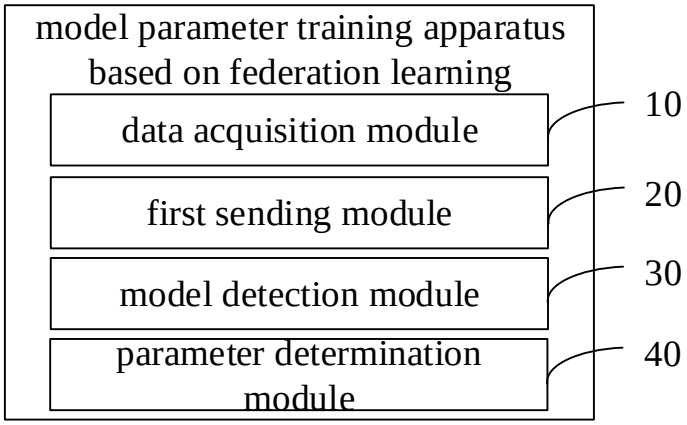
model parameter training apparatus based on federation learning
data acquisition module
first sending module
model detection module
parameter determination module
10
20
30
40

FIG. 6