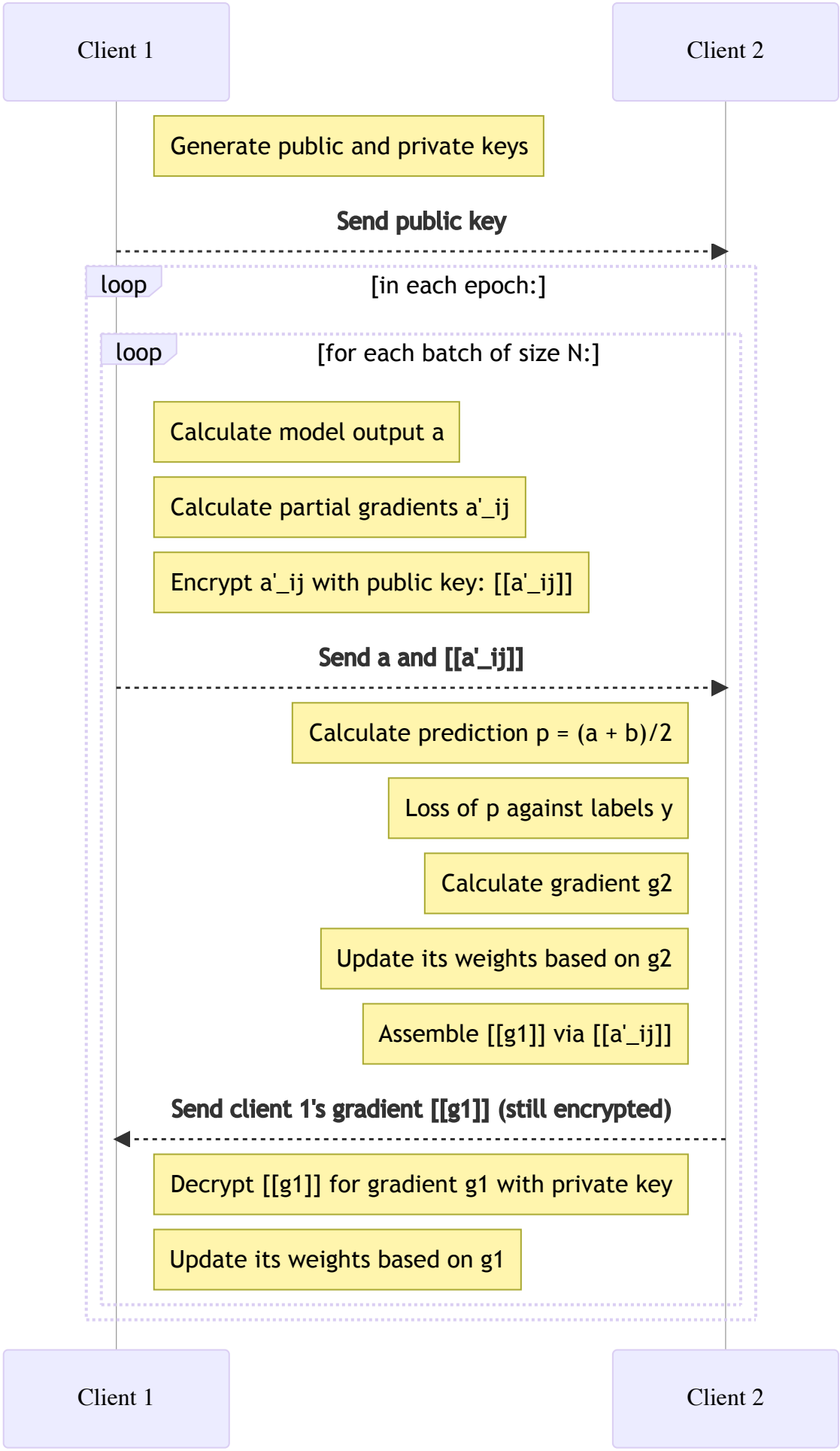
Client 1
Client 2
Generate public and private keys
Send public key
loop
[in each epoch:]
loop
[for each batch of size N:]
Calculate model output a
Calculate partial gradients a'_ij
Encrypt a'_ij with public key: [[a'_ij]]
Send a and [[a'_ij]]
Calculate prediction p = (a + b)/2
Loss of p against labels y
Calculate gradient g2
Update its weights based on g2
Assemble [[g1]] via [[a'_ij]]
Send client 1's gradient [[g1]] (still encrypted)
Decrypt [[g1]] for gradient g1 with private key
Update its weights based on g1
Client 1
Client 2