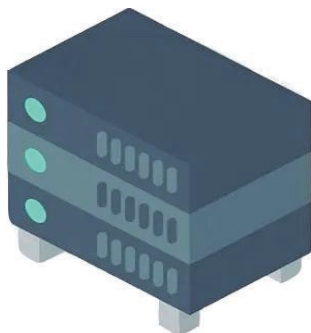




Public
dataset



Server

normal gradient: $\Delta \omega_i$

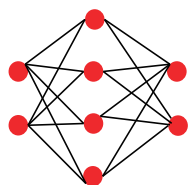
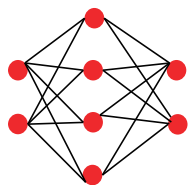
malicious gradient: *

$\Delta \omega_1$

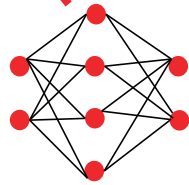
$\Delta \omega_2$

*

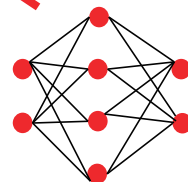
$\Delta \omega_n$



...



...



Client 1

Client 2

Client k
(Malicious
participants)

Client n