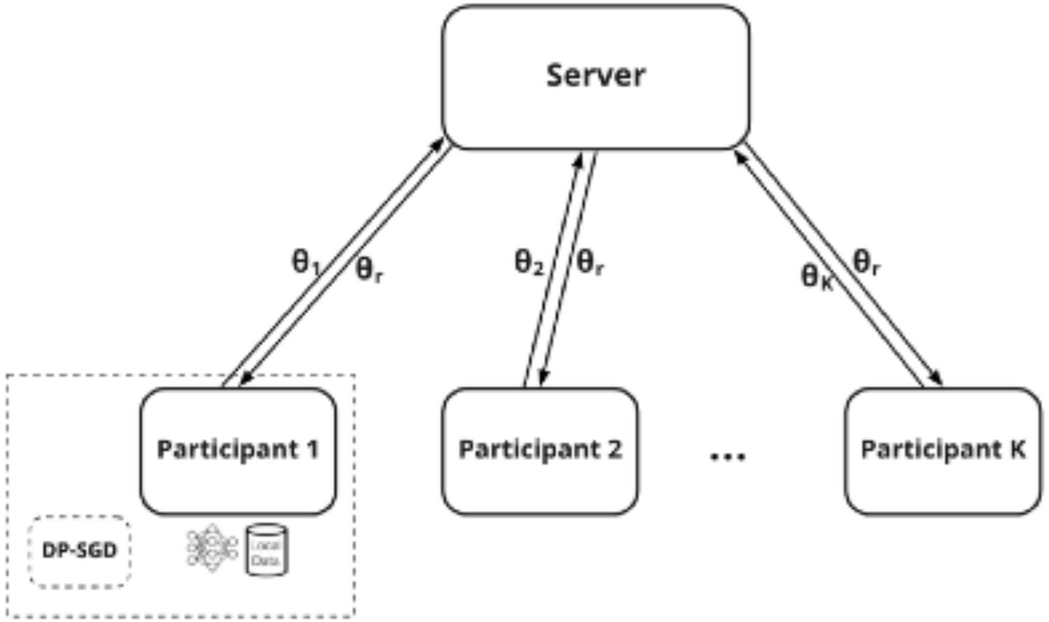
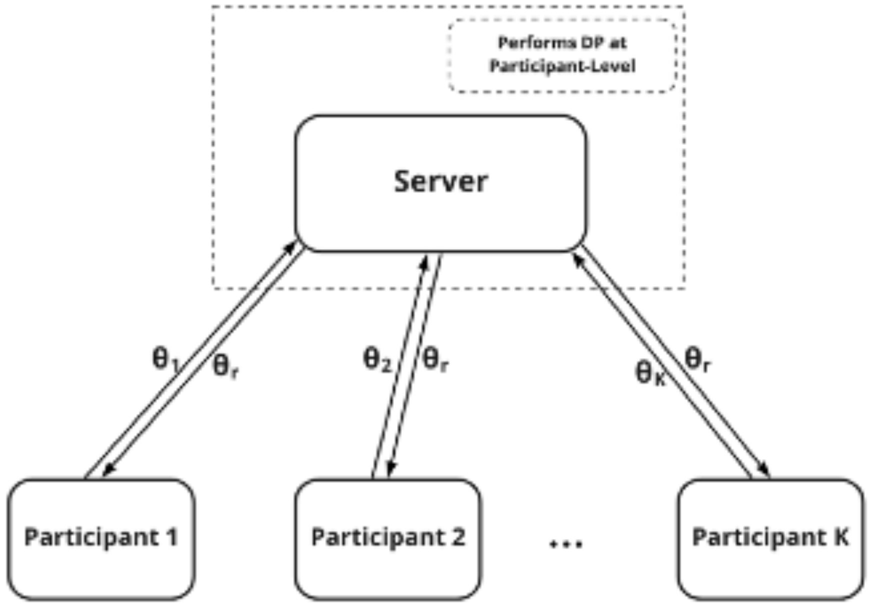
Local vs Central DP

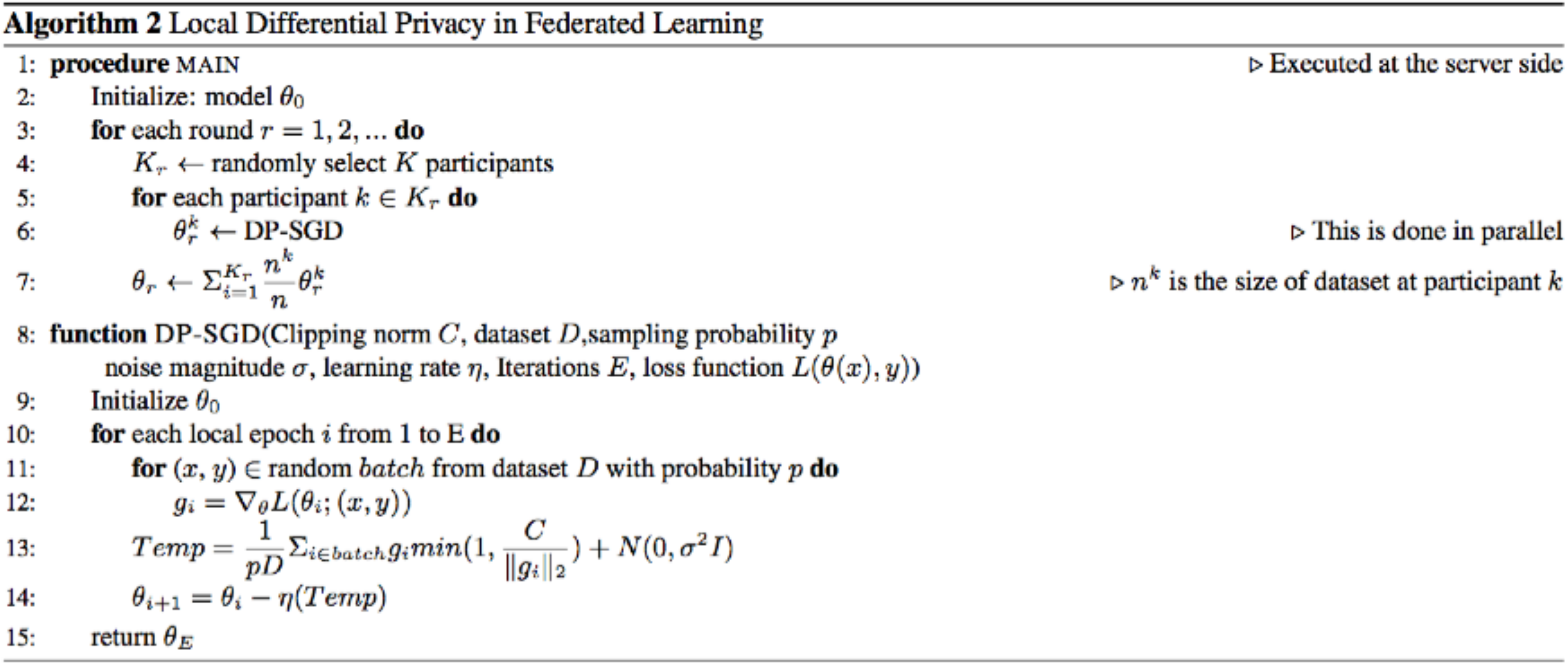


Local Differential Privacy
(LDP)



Central Differential Privacy
(CDP)

Local DP



Algorithm 2 Local Differential Privacy in Federated Learning

```
procedure MAIN                                                        ▷ Executed at the server side
    Initialize: model $\theta_0$
    for each round $r = 1, 2, \ldots$ do
        $K_r \leftarrow$ randomly select $K$ participants
        for each participant $k \in K_r$ do
            $\theta_r^k \leftarrow$ DP-SGD                             ▷ This is done in parallel
        $\theta_r \leftarrow \Sigma_{i=1}^{K_r} \frac{n^k}{n} \theta_r^k$       ▷ $n^k$ is the size of dataset at participant $k$
function DP-SGD(Clipping norm $C$, dataset $D$,sampling probability $p$
      noise magnitude $\sigma$, learning rate $\eta$, Iterations $E$, loss function $L(\theta(x), y)$)
    Initialize $\theta_0$
    for each local epoch $i$ from 1 to E do
        for $(x, y) \in$ random $batch$ from dataset $D$ with probability $p$ do
            $g_i = \nabla_\theta L(\theta_i; (x, y))$
        $Temp = \frac{1}{pD} \Sigma_{i \in batch} g_i min(1, \frac{C}{\|g_i\|_2}) + N(0, \sigma^2 I)$
        $\theta_{i+1} = \theta_i - \eta(Temp)$
    return $\theta_E$
```