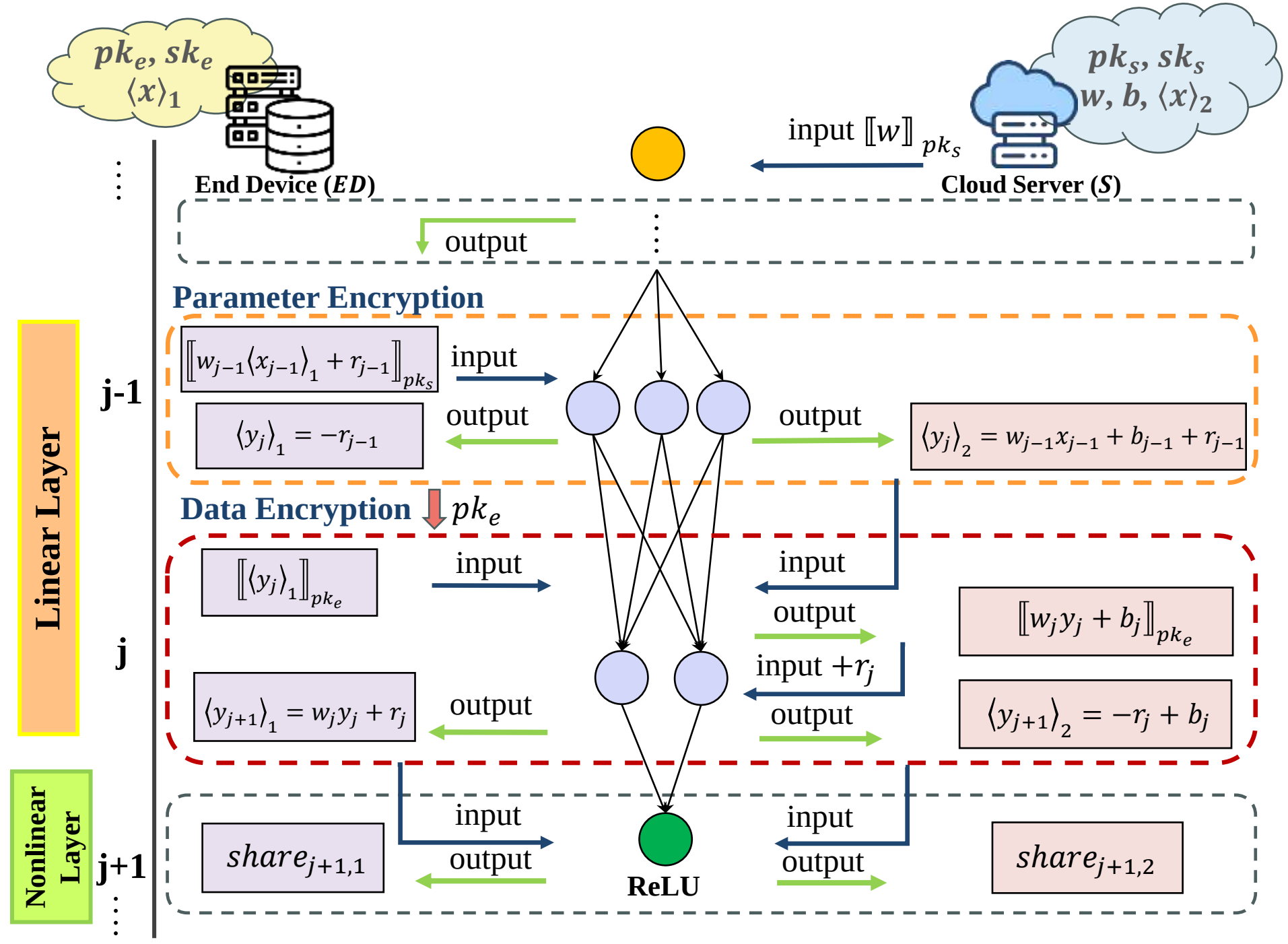
pk_e, sk_e
$\langle x \rangle_1$
End Device (ED)
pk_s, sk_s
$w, b, \langle x \rangle_2$
Cloud Server (S)
input $[\![w]\!]_{pk_s}$
output
Parameter Encryption
Linear Layer
j-1
$[\![w_{j-1}\langle x_{j-1}\rangle_1 + r_{j-1}]\!]_{pk_s}$
input
$\langle y_j \rangle_1 = -r_{j-1}$
output
output
$\langle y_j \rangle_2 = w_{j-1}x_{j-1} + b_{j-1} + r_{j-1}$
Data Encryption
pk_e
j
$[\![\langle y_j \rangle_1]\!]_{pk_e}$
input
input
output
$[\![w_j y_j + b_j]\!]_{pk_e}$
input $+r_j$
$\langle y_{j+1} \rangle_1 = w_j y_j + r_j$
output
output
$\langle y_{j+1} \rangle_2 = -r_j + b_j$
Nonlinear Layer
j+1
input
$share_{j+1,1}$
output
ReLU
input
output
$share_{j+1,2}$