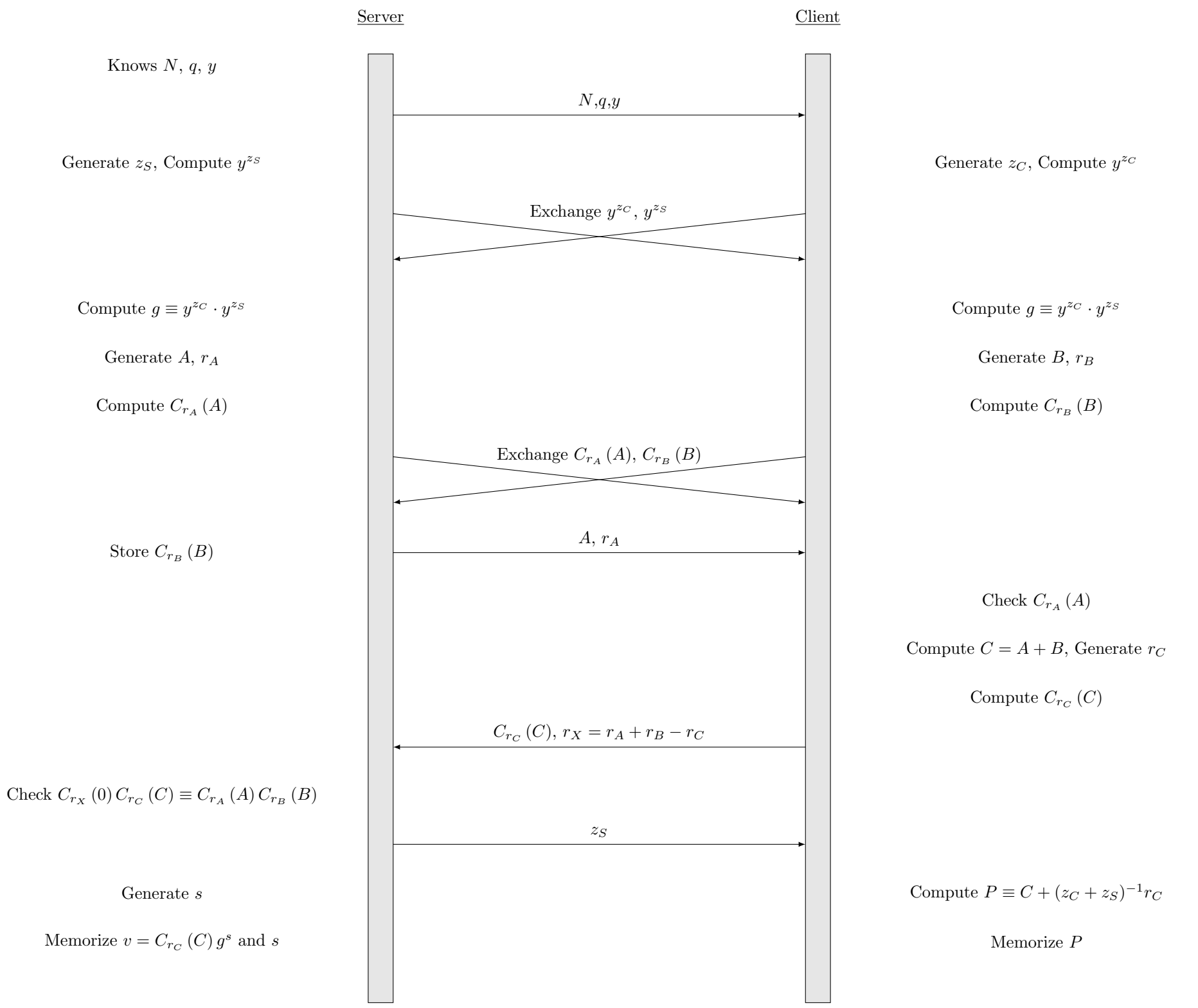
Server
Client
Knows N, q, y
N,q,y
Generate z_S, Compute y^{z_S}
Generate z_C, Compute y^{z_C}
Exchange y^{z_C}, y^{z_S}
Compute $g \equiv y^{z_C} \cdot y^{z_S}$
Compute $g \equiv y^{z_C} \cdot y^{z_S}$
Generate A, r_A
Generate B, r_B
Compute $C_{r_A}(A)$
Compute $C_{r_B}(B)$
Exchange $C_{r_A}(A)$, $C_{r_B}(B)$
A, r_A
Store $C_{r_B}(B)$
Check $C_{r_A}(A)$
Compute $C = A + B$, Generate r_C
Compute $C_{r_C}(C)$
$C_{r_C}(C)$, $r_X = r_A + r_B - r_C$
Check $C_{r_X}(0)\, C_{r_C}(C) \equiv C_{r_A}(A)\, C_{r_B}(B)$
z_S
Generate s
Compute $P \equiv C + (z_C + z_S)^{-1} r_C$
Memorize $v = C_{r_C}(C)\, g^s$ and s
Memorize P