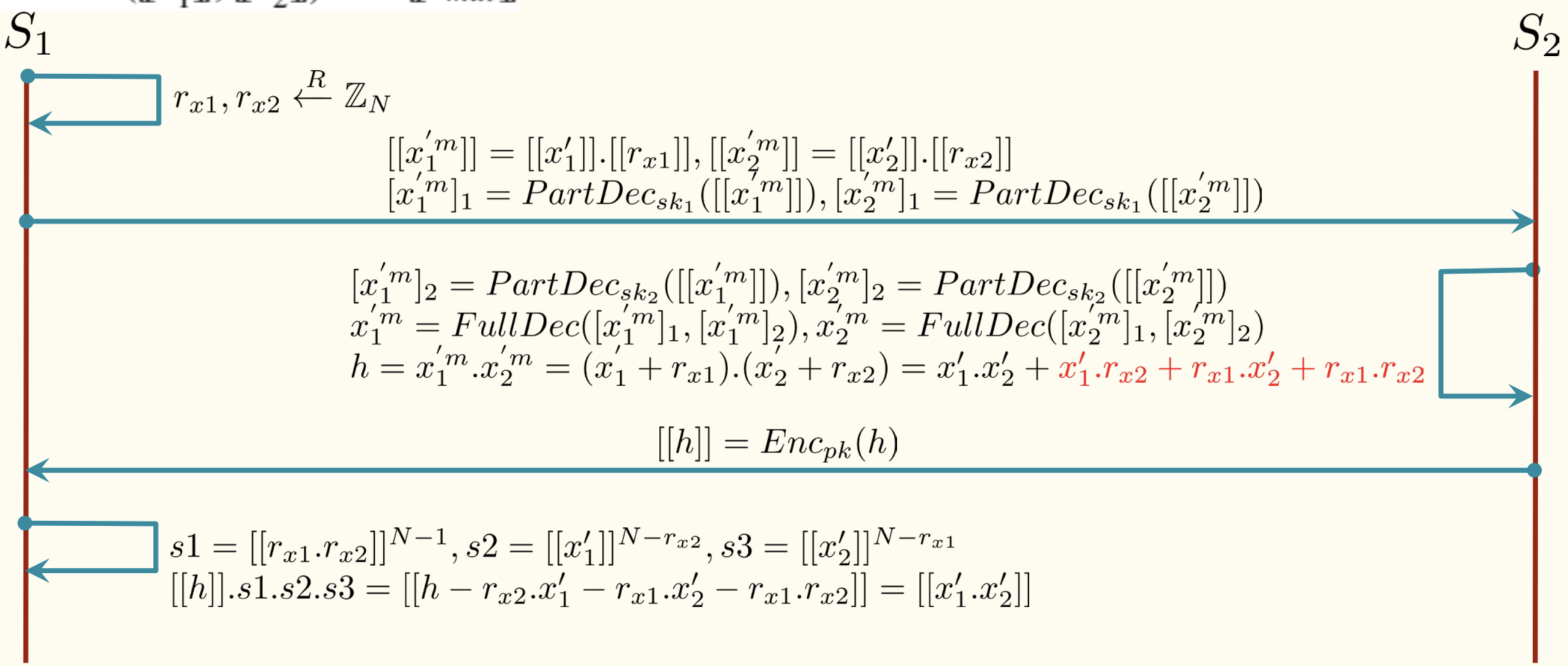
S_1
S_2
$r_{x1}, r_{x2} \xleftarrow{R} \mathbb{Z}_N$
$[[x_1'^m]] = [[x_1']].[[r_{x1}]], [[x_2'^m]] = [[x_2']].[[r_{x2}]]$
$[x_1'^m]_1 = PartDec_{sk_1}([[x_1'^m]]), [x_2'^m]_1 = PartDec_{sk_1}([[x_2'^m]])$
$[x_1'^m]_2 = PartDec_{sk_2}([[x_1'^m]]), [x_2'^m]_2 = PartDec_{sk_2}([[x_2'^m]])$
$x_1'^m = FullDec([x_1'^m]_1, [x_1'^m]_2), x_2'^m = FullDec([x_2'^m]_1, [x_2'^m]_2)$
$h = x_1'^m.x_2'^m = (x_1' + r_{x1}).(x_2 + r_{x2}) = x_1'.x_2' + x_1'.r_{x2} + r_{x1}.x_2' + r_{x1}.r_{x2}$
$[[h]] = Enc_{pk}(h)$
$s1 = [[r_{x1}.r_{x2}]]^{N-1}, s2 = [[x_1']]^{N-r_{x2}}, s3 = [[x_2']]^{N-r_{x1}}$
$[[h]].s1.s2.s3 = [[h - r_{x2}.x_1' - r_{x1}.x_2' - r_{x1}.r_{x2}]] = [[x_1'.x_2']]$