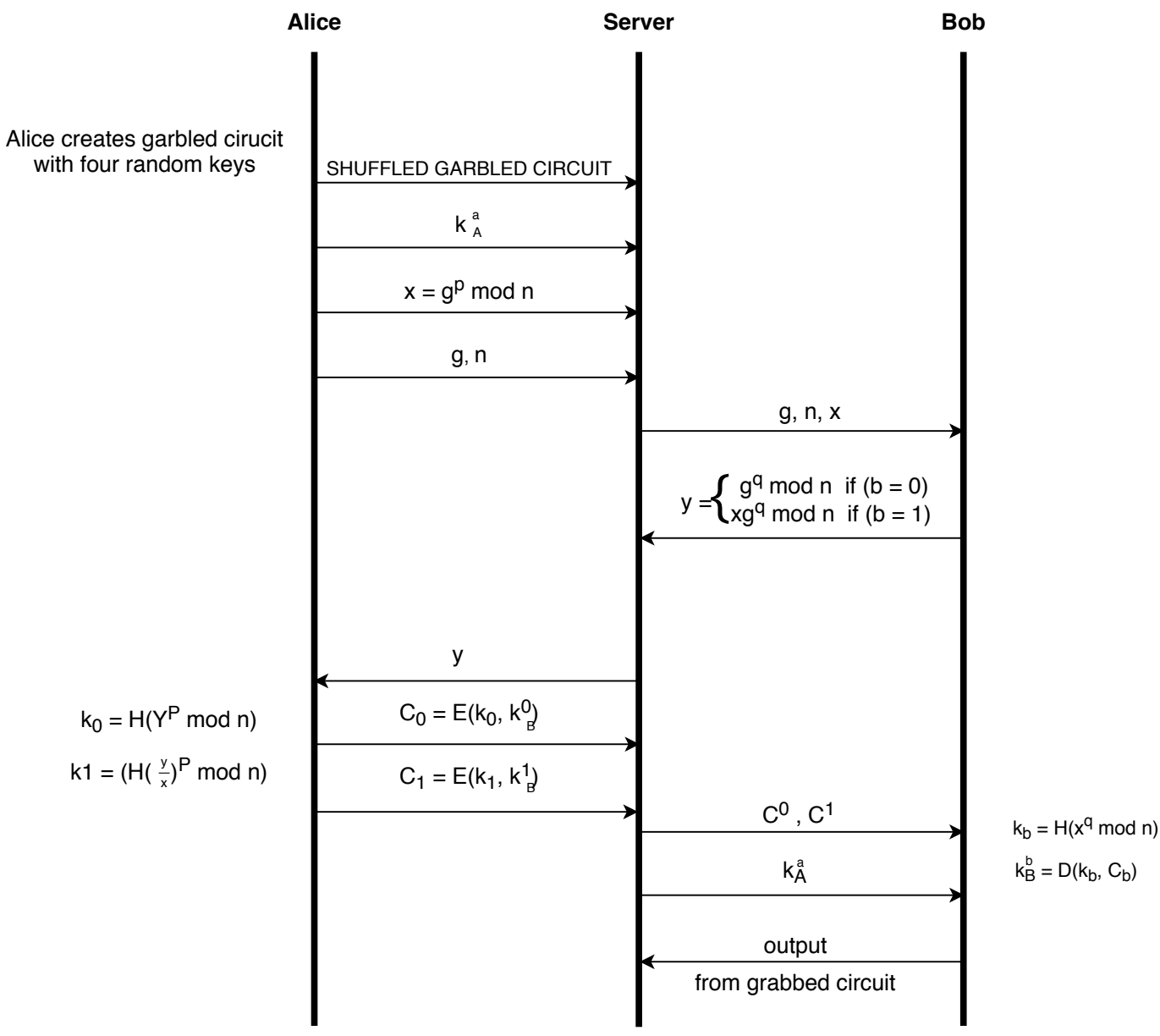
Alice
Server
Bob
Alice creates garbled cirucit with four random keys
SHUFFLED GARBLED CIRCUIT
k_A^a
$x = g^p \bmod n$
g, n
g, n, x
$y = \begin{cases} g^q \bmod n & \text{if } (b = 0) \\ xg^q \bmod n & \text{if } (b = 1) \end{cases}$
y
$k_0 = H(Y^P \bmod n)$
$C_0 = E(k_0, k_B^0)$
$k1 = (H(\frac{y}{x})^P \bmod n)$
$C_1 = E(k_1, k_B^1)$
C^0, C^1
$k_b = H(x^q \bmod n)$
$k_B^b = D(k_b, C_b)$
k_A^a
output
from grabbed circuit