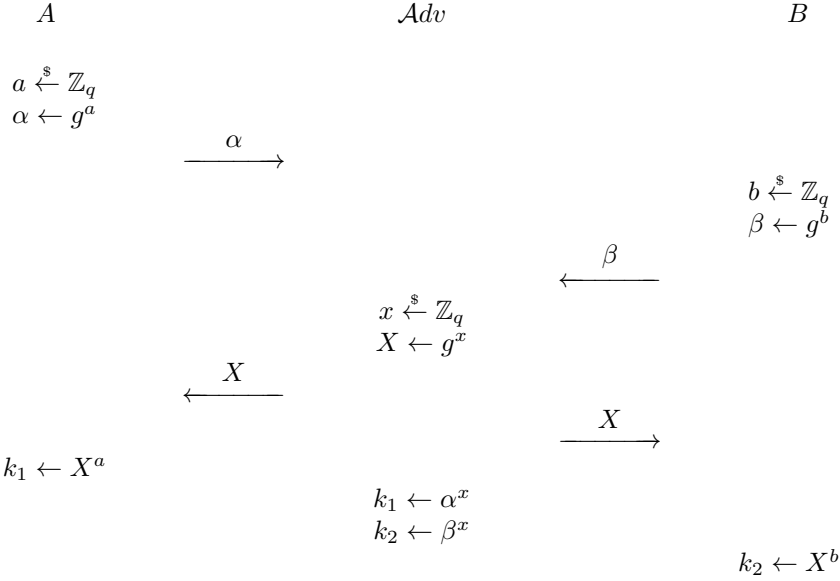
A
Adv
B
a ←$ Z_q
α ← g^a
α
b ←$ Z_q
β ← g^b
β
x ←$ Z_q
X ← g^x
X
X
k_1 ← X^a
k_1 ← α^x
k_2 ← β^x
k_2 ← X^b