



Alice

$(sk_A, pk_A)$



Bob

$(sk_B, pk_B)$