(2)

|Pr[W0] – Pr[W1]| = DDHadv[Bddh, G]

If DDH assumption does not hold in G, DDHadv[Bddh, G] is not negligible.

Thus, adversary can distinguish whether a tuple (u, v, w) is DH-triple or not.

Therefore, SSadv[A, EMEG] = 1.

(3)

c1 ← E(pk, m1) = uαm1

c2 ← E(pk, m2) = u βm2

Thus c1c2 = uαm1u βm2 = uα+β m1m2

c ← E(pk, m1m2) = uα+βm1m2

Therefore c1c2 equals to c.

(4)

According to the solution in the previous question, we already have a solution for E(pk, m1) \* E(pk, m2) = E(pk, m1 \* m2). We then replace m with gm.

c1 ← E(pk, gm1) = uαgm1

c2 ← E(pk, gm2) = u βgm2

With this transformation, E(pk, gm1)E(pk, gm2) = E(pk, gm1gm2) = E(pk, gm1+m2). Now we have an additive homomorphic property.