CSCI971 Modern Cryptography Assignment 8

Author: Weijian Ye

1.

Alice

Bob

(m2, gk)

m ← M

p ← Zq

m1 ←

m3 ← (m2)/(gkgp)

k ← K

m2 ← m1K

m1

m1 ← H(m)gp

m3 = [H(m)gp]k/(gkgp) = H(m)k

2.

（1）

DDH Challenger

Adversary A

u, v, w

(v, c)

(m0, m1)

B

b ← {0, 1}

u

c ← wmb

Between A and B, there is SSadv\*[A, EMEG] = | Pr[W0] – 1/2|

Between DDH challenger and B, there is DDHadv[Bddh, G] = |Pr[W0] – Pr[W1]|

There is also Pr[W1] = ½

According to equations above, SSadv\*[A, EMEG] = DDHadv[Bddh, G]

Thus, EMEG is semantically secure if DDH assumption holds in G.

α, β ← Zq

γ ← Zq

u ← gα

v ← gβ

w ← gγ

b’