CSCI971 Modern Cryptography Assignment 9

author: Weijian Ye

a)

e(H(m), u) = e(H(m), g1α) = e(H(m)α, g1) = e(σ, g1)

b)

Challenger

(u0, u1, v0, g1)

if j != i\*

pj←Zq

H(mj)←g0pj

if i != i\*

pi←Zq

σi←u0pi

if e(h(m), u) == e(σ, g1)

z0’← σ

‘accept’

There is a possibility for A to output (mi\*, σ) where i\* is indicated by B. In this case, σ = H(m)α = H(mi\*)α = v0α = z0 .

We can draw a conclusion that SIGroadv[A, Sbls] ≤ C(Qs + 1) coCDHadv[β, e] .

z0’

Shape

Description automatically generated with low confidence

(m, σ)

σi

H(mj)

mi

α, β ← Zq

u0 ← g0α

u1 ← g1α

v0 ← g0β

z0 ← g0αβ

A

B

i\* ← {1, …, qs}

}

Shape

Description automatically generated with low confidenceShape

Description automatically generated with low confidence

mj

u1