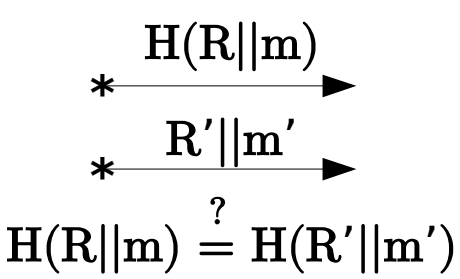
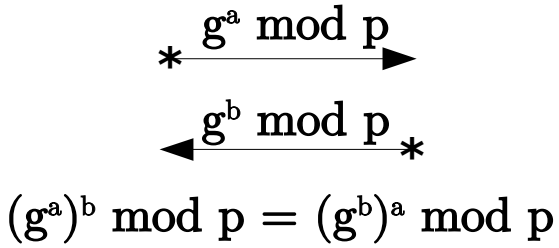
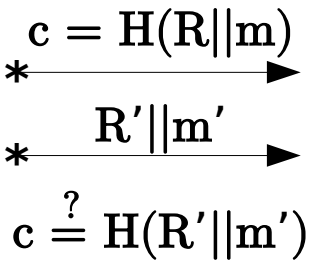
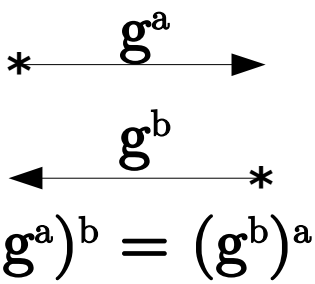
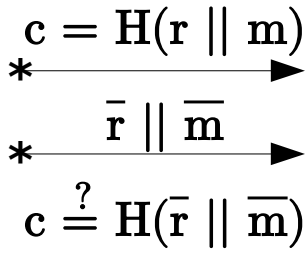
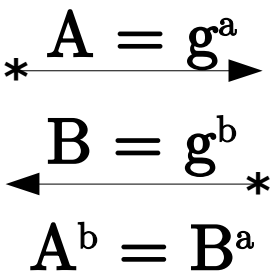

H(R||m)
R′||m′
H(R||m) ?= H(R′||m′)

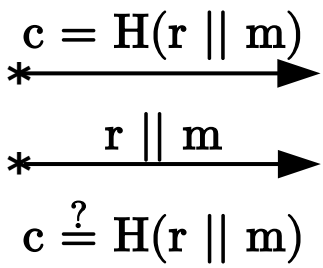

g^a mod p
g^b mod p
(g^a)^b mod p = (g^b)^a mod p

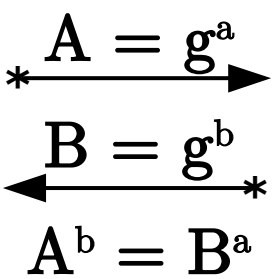

c = H(R||m)
R′||m′
c ?= H(R′||m′)


g^a
g^b
(g^a)^b = (g^b)^a


c = H(r || m)
r̄ || m̄
c ?= H(r̄ || m̄)


A = g^a
B = g^b
A^b = B^a


c = H(r || m)
r || m
c ?= H(r || m)


A = g^a
B = g^b
A^b = B^a