Cryptographic Protocols

Session 9 - Sigma Protocols II

1. Implement a sigma protocol showing that lifted Elgamal ciphertext encrypts 0, that is, sigma protocol should be for the following relation:
   \[ \mathcal{R}_0 := \{ (c, r) \mid c = (h^r, g^r) \} . \]

2. Implement a sigma protocol showing that lifted Elgamal ciphertext encrypts 1, that is, sigma protocol should be for the relation:
   \[ \mathcal{R}_1 := \{ (c, r) \mid c = (gh^r, g^r) \} . \]

3. Implement a sigma protocol showing that lifted Elgamal ciphertext encrypts either 0 or 1, that is, sigma protocol should be for the relation:
   \[ \mathcal{R}_{0\lor1} := \{ (c, (b, r)) \mid c = (g^b h^r, g^r) \land b \in \{0, 1\} \} . \]