ElGamal is sem. secure under Hash-DH

Dan Boneh