



NOTE: This involves large computational cost to increase the attack cost. This also guarantees the forward secrecy.