1. (Lossy Encryption) Let \( (\text{Gen}, E, D) \) be a public key encryption scheme. In this problem we define a new property for PKE schemes that we call “lossy encryption”. We say that a scheme \( (\text{Gen}, E, D) \) is **lossy** if there exists an algorithm \( \text{LossyGen}(1^n) \) which generates a “lossy” public key without a secret key such that the following two properties are satisfied:

1. A lossy public key is computationally indistinguishable from a public key generated by \( \text{Gen} \): \( PK \approx PK' \). More formally, for any PPT adversary \( A \) it holds:
   \[
   | \Pr[A(PK) = 1 | (PK, SK) \leftarrow \text{Gen}(1^n)] - \Pr[A(PK') = 1 | PK' \leftarrow \text{LossyGen}(1^n)] | \leq \text{negl}(n)
   \]

2. For any lossy public key \( PK' \leftarrow \text{LossyGen}(1^n) \), encrypting any message using \( PK' \) produces ciphertexts that have identical distribution. Namely, for any \( PK' \leftarrow \text{LossyGen}(1^n) \), and any pair of messages \( m_0, m_1 \in M \), we have \( (PK', E(PK', m_0)) \equiv (PK', E(PK', m_1)) \).

Intuitively, notice that this second property is saying that encrypting using the lossy public key completely loses information about the original plaintext, and thus it is not possible to decrypt.

(a) (5 points) Prove that if an encryption scheme is lossy according to the definition provided above, then the scheme is also IND-CPA-secure.

(b) (3 points) Describe a decryption algorithm.

(c) (8 points) Second, prove that the scheme described above (together with the decryption algorithm that you obtained from part b) is a lossy public key encryption based on the DDH assumption. Namely, first describe a lossy key generation algorithm \( \text{LossyGen}(1^n) \) and then show that it satisfies both properties (1) and (2). Deduce that the scheme is IND-CPA-secure.

(d) (5 points) Although the lossy property may be nice and useful in some contexts, this is not necessary to prove that the scheme is IND-CPA-secure. Prove directly that this scheme is IND-CPA-secure under the DDH assumption; namely,

\[
(g_0, g_1, h_0, h_1, g_0^{r_0}, h_0^{r_0}) \approx (g_0, g_1, h_0, h_1, g_1^{r_1}, h_1^{r_1})
\]

A small hint (ID 51599)

---

1From Dodis