Homework 10

Homework is due by **11pm of Nov 25**. Send by email to both "regev" (under the cs.nyu.edu domain) and "des480" (under the nyu.edu domain) with subject line "CSCI-GA 3210 Homework 10" and name the attachment "YOUR NAME HERE HW10.tex/pdf". There is no need to print it. Start early!

1. *(Lossy Encryption)*[1] Let (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 (Gen, E, D) is *lossy* if there exists an algorithm $LossyGen(1^n)$ which generates a "lossy" public key PK' (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 Gen: $PK \approx PK'$. More formally, for any PPT adversary A it holds:

    $$|\Pr[A(PK) = 1|(PK, SK) \leftarrow Gen(1^n)] - \Pr[A(PK') = 1|PK' \leftarrow LossyGen(1^n)]| \leq \text{negl}(n)$$

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

    A small hint (ID 51588)

    Consider the following scheme as a potential candidate for being a lossy public key encryption. $Gen(1^n)$ chooses a random n-bit large "safe" prime p (i.e., $p = 2q + 1$ for a large prime q) and chooses two random generators g_0, g_1 of $G = QR_p$ (recall that QR_p is the subgroup of quadratic residues in $\mathbb{Z}_p^*$). Next, it chooses two random (but distinct) values $x_0, x_1 \in \mathbb{Z}_q$, computes $h_0 = g_0^{x_0}$, $h_1 = g_1^{x_1}$, and outputs $PK = (p, g_0, g_1, h_0, h_1)$ and $SK = (x_0, x_1)$.

    To encrypt a 1-bit message $m \in \{0, 1\}$, $E(PK, m)$ proceeds as follows: choose a random $r \in \mathbb{Z}_q$ and output $C = (g_m^r, h_m^r)$.

    (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 $LossyGen(1^n)$ and then show that it satisfies both properties (1) and (2). Deduce that the scheme is IND-CPA-secure. A hint for 2 points (ID 51589)

    (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)

[1] From Dodis