Homework 0

CSE 208: Advanced Cryptography *(Winter 2017)*

Instructor: Daniele Micciancio

Due: Tuesday January 17, at the beginning of class.

Grading: This is a calibration homework, meant to test your cryptography background, as acquired in an introductory graduate level cryptography course, and your ability to present it in a clear and concise way. You are not required to type your solutions, but your work will be evaluated both for correctness and clarity. Your solution will be graded on an A/B/C scale, with A="correct and well written solution", B="Mostly ok solution, but you can/should do better if you want to pass with a good grade", C="Inadequate for graduate level class. Either you miss the necessary prerequisite/background to take this course, or you need to put substantially more effort on the assignments." Don't confuse clarity with level of detail. A very detailed solution can be unclear and hard to read. Similarly, a well written solution may leave out the most mundane details of the proof (e.g., probability calculations) to the reader, and still provide a solution that is both clear and concise. While deciding how much to write is left primarily to your own judgment, as an indication, I expect a good solution to each of the two problems below can be written in about one page.

Multimessage-security

Consider the following definition of multi-message security for public key encryption.

Let `(KeyGen,Enc,Dec)` be a public key encryption (PKE) scheme as defined in lecture and satisfying the usual correctness requirement `Dec(sk,Enc(pk,m)) = m` for all `(pk,sk) <- KeyGen(t)`.

A *left-right encryption oracle* is a randomized algorithm $LR^b_{pk}(m_0, m_1) = Enc(pk, m_b)$ parametrized by a bit $b \in \{0, 1\}$ and public key pk that on input two messages m_0, m_1, outputs the encryption (under pk) of one of them, selected according to the bit b.

An adversary in the multi-message IND-CPA definition of security for PKE is an algorithm $A^{LR}(pk)$ that takes a public key pk as input, and it is given oracle access to an left-right encryption oracle LR. For any bit $b \in \{0, 1\}$, define the output of the adversary in the multi-message IND-CPA game as

$$Out_b[A] = \{A^{LR^b_{pk}}(pk) \mid (pk, sk) \leftarrow KeyGen(t)\}$$

Definition: A PKE scheme is n-IND-CPA secure if for any PPT adversary A making at most n queries to its LR-oracle, the probability $|Pr\{Out_b[A] = b \mid b \leftarrow \{0,1\}\}|$ is negligible in the security parameter t.

A scheme is multi-message IND-CPA secure if it is n-IND-CPA secure for any n polynomial in the security parameter t.

Notice that the IND-CPA security definition given in class corresponds to 1-IND-CPA, i.e., the special case where A is allowed to make exactly one query to the LR-oracle. So, clearly, any PKE scheme that satisfies the n-IND-CPA security definition is also IND-CPA secure according to the definition given in class.

Problem 1: Show that the converse is also true, i.e., any 1-IND-CPA secure PKE scheme is also n-IND-CPA secure. *Hint: show how any adversary attacking n-IND-CPA security with advantage ε can be converted into an adversary attacking 1-IND-CPA security with advantage ϵ/n.*

Secret Key Encryption

Now consider the case of private key encryption. A private key encryption scheme is defined just like a PKE, with the only difference that pk=sk, i.e., the same key is used both to encrypt and decrypt. n-IND-CPA security is defined similarly, with the only difference that the adversary is not given the key $pk = sk$ as input. In other words, $sk \leftarrow KeyGen(t)$ outputs just one key, and the output of an adversary A in the security game is

$$Out_b[A] = \{A^{LR^b_{sk}}() \mid sk \leftarrow KeyGen(t)\}$$

Definition:
A private key encryption scheme is n-IND-CPA secure if for any PPT adversary A making at most n queries to its LR-oracle, the probability $|Pr\{Out_b[A] = b \mid b \leftarrow \{0,1\}\}|$ is negligible in the security parameter t.

Problem 2: Prove that in the case of private-key encryption, 1-IND-CPA security does not imply n-IND-CPA security (even for $n = 2$). Specifically, give a private key encryption scheme that is 1-IND-CPA secure, but not 2-IND-CPA secure.