Security Models

2020/2021

P. Lafourcade and L.Robert

Session 1

Exercise 1 (Negligible functions)
Let f and g be two negligible functions. Prove that:

1. $f \cdot g$ is negligible.
2. For any $k > 0$, f^k is negligible.
3. For any $\lambda, \mu \in \mathbb{R}$, $\lambda, \mu > 0$, $\lambda \cdot f + \mu \cdot g$ is negligible.

Exercise 2 (DL, CDH, DDH assumptions)
Recall DL, CDH, and DDH assumptions and prove that:

1. Solving DL $\Rightarrow$ Solving CDH.
2. Solving CDH $\Rightarrow$ Solving DDH.

Exercise 3 (Deterministic Asymmetric Encryption Scheme)
Let $\Pi = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a deterministic asymmetric encryption scheme. Prove that Π is not IND-CPA.

Exercise 4 (Indistinguishability security)
Let E be an encryption that is IND-CPA and H be a public hash function. We define the following encryption $\mathcal{E}$ as follows: $\mathcal{E}(x) = E(x)||H(x)$, where $||$ denotes the concatenation of bit-strings.

Show that the encryption $\mathcal{E}$ is not IND-CPA secure.

Exercise 5 (One-way security)
Let f be a one-way function, we construct the encryption E as follows:

- Pick a random value x in the domain of f.
- The encryption of m is $\langle f(x), x \oplus m \rangle$

Prove that: if f is a one-way function, then E is a OW-CPA encryption scheme.

Exercise 6 (Prime order groups)
Usually, cyclic groups are considered for which discrete logarithm and DH problems are believed to be hard. There are several reasons we prefer prime order groups over composite ones. A first reason is that discrete logarithm is harder in prime order groups (but it is still hard in non-prime order groups). A second reason is because finding generator is trivial (why?). A final reason applies when DDH should be hard. A necessary condition for the DDH to be hard is that $g^{x_1 x_2}$ should be indistinguishable from a random group element. The goal of this exercise is to show that this is (almost) true.

Let G be a group of prime order q with generator g.

1. If x_1, x_2 are chosen uniformly at random from $\mathbb{Z}_q$, show that:
$$Pr[g^{x_1 x_2} = 1] = \frac{2}{q} - \frac{1}{q^2}$$
2. For any $y \in G, y \neq 1$, show that:
$$Pr[g^{x_1 x_2} = y] = \frac{1}{q} - \frac{1}{q^2}$$
3. Conclude by comparing the previous results with the uniform distribution over G when $||q|| = n$.

Note that using a prime order grouop is neither necessary nor sufficient for the DDH problem to be hard.