Cryptography, winter 2015/16

MICHAEL NÜSKEN, SIMON SCHNEIDER

4. Exercise sheet
Hand in solutions until Saturday, 28 November 2015, 12:00

Exercise 4.1 (OW-KOA). (10 points)

One-wayness game G^{OW}.

1. Prepare a key $k \leftarrow \mathrm{KeyGen}(1^\kappa)$ in $\mathcal{K}$.
2. Choose a plaintext $m \xleftarrow{\text{⚄}} \mathcal{M}$ uniformly random.
3. Prepare a *one-time* oracle $\mathcal{O}_{\mathrm{Test}}$ that when called with no input the oracle returns $c \leftarrow \mathrm{Enc}_k(m)$.
4. Call the attacker $\mathcal{A}$ with input 1^κ and the oracle $\mathcal{O}_{\mathrm{Test}}$. Await a guess $m' \in \mathcal{M}$.
5. If $m = m'$ then ACCEPT else REJECT .

(i) Determine the success probability of the guessing attacker $\widetilde{\mathcal{A}}$ that merely picks $m' \xleftarrow{\text{⚄}} \mathcal{M}$ uniformly random. $\boxed{4}$

(ii) Prove that every indistinguishable encryption scheme is also one-way secure, ie. each probabilistic polynomial-time attacker has at most a negligible advantage in winning the game G^{OW}. $\boxed{6}$

Exercise 4.2 (Negligible or significant?). (4 points)

Decide which of the following functions are negligible or significant. $\boxed{4}$

f	$\frac{1}{\sqrt{\log_2 n}}$	$2^{-\sin n \cdot \log_2 n}$	$n^3 2^{-n}$	$\frac{\log_2 n}{n^4}$	2^{-n^2}	$2^{-\frac{1}{n}}$	$2^{-\frac{\log_2 n}{\log_2 \log_2 n}}$	$2^{-\frac{\log_2 n}{\sin n}}$
negligible?								
significant?								

Exercise 4.3 (Amplification — or: A little bit better than guessing is enough). (3+11 points)

Think of a boolean variable T and an algorithm $\mathcal{A}$ with output A and a probability slightly better than guessing to determine the value of T, ie.

$$p = \text{prob}\,(A = T) > \frac{1}{2}.$$

Imagine a new algorithm $\mathcal{B}$ which calls $\mathcal{A}$ independently m times and outputs B as the majority of the $\mathcal{A}$s — returning failure in the event of a draw.

$\boxed{3}$ (i) Compute for $m = 3$ the probability

$$p_3 = \text{prob}\,(B = T)$$

that B succeeds.

$\boxed{+4}$ (ii) Prove that

$$\text{prob}(B = T) \geq \sum_{m/2 < i \leq m} \binom{m}{i} p^i (1-p)^{m-i}$$

and give a simple —but still useful— lower bound for the sum.

Hint: Chernoff.

$\boxed{+3}$ (iii) How many repetitions, m, do you need for $p = 0.6, 0.7, 0.8$ in order to guarantee prob $(B = T) > 0.9$?

$\boxed{+4}$ (iv) Let $p = \frac{1}{2} + \frac{1}{n}$. Determine a number of repetitions such that

$$\text{prob}\,(B = T) > 1 - e^{-cn}$$

for some constant $c > 0$.