ETH Zürich, D-INFK
Spring 2018

Prof. Ueli Maurer
Christian Badertscher
Fabio Banfi

Cryptography Foundations

Exercise 7

7.1 Search Problems

Goal: *Understand the random experiment of an algorithm trying to solve a search problem.*

a) Describe the setting of a (probabilistic) algorithm A trying to solve a search problem $(\mathcal{X}, \mathcal{W}, Q, \mathsf{P}_X)$ as a random experiment. What are the random variables in this random experiment? How is the success probability of A defined?

b) Let A be an algorithm with success probability $\alpha \in (0, 1]$ for some search problem $(\mathcal{X}, \mathcal{W}, Q, \mathsf{P}_X)$ such that Q can (efficiently) be computed by an algorithm. Let the algorithm A' be defined as follows: Given an instance $x \in \mathcal{X}$, it first invokes A on input x to retrieve w. If $Q(x, w) = 1$, A' returns w. Otherwise, it invokes A again on input x to retrieve w' and returns w'. Find the best lower bound on the success probability of A'.

c) Suppose there is an algorithm A that solves the discrete logarithm problem with probability $\alpha \in (0, 1]$. Describe an algorithm A' (that uses A) such that the success probability of A' exceeds the one of A.

Hint: Given a group element g^x how can you obtain a "uniform but related" element g^y?

d) Why does the technique used in part **c)** not apply in general?

7.2 Reductions Related to Discrete Logarithms

Goal: *Devise a reduction from the discrete logarithm problem to the computational Diffie-Hellman problem.*

Let $\mathbb{G} = \langle g \rangle$ be a cyclic group of prime order q such that $q = 2^k + 1$ for some $k \in \mathbb{N}$ and the group operation can be efficiently computed.

Suppose you are given an oracle that solves the computational Diffie-Hellman problem in $\mathbb{G}$ with probability 1 for every query. Devise an efficient algorithm that uses this oracle to solve the discrete logarithm problem in $\mathbb{G}$ with probability 1 for every group element.

Hint: For $y = g^x \neq 1$, the discrete logarithm x of y is an element of $\mathbb{Z}_q^*$. Use the results from Exercise **3.3 d)** and assume that a generator of $\mathbb{Z}_q^*$ is known.

7.3 Properties of the Statistical Distance

Goal: *We show (1) that a probabilistic function (or algorithm) cannot increase the statistical distance of two random variables, and (2) that uniform distributions over two intervals of similar size are statistically close.*

a) Let $\mathcal{X}$ and $\mathcal{Y}$ be finite sets and let X and X' be random variables over $\mathcal{X}$. Further let A be a random variable over the set of functions $\mathcal{X} \to \mathcal{Y}$ such that A and X are independent and A and X' are independent. Show that

$$\delta\big(A(X), A(X')\big) \leq \delta\big(X, X'\big).$$

b) Let I be some set and $J \subseteq I$. Further let X be uniformly distributed over I and let Y be uniformly distributed over J. Show that

$$\delta(X, Y) = 1 - \frac{|J|}{|I|}.$$

Discussion of solutions:

16/17.4.2018 (Task 7.1 and Task 7.2)

23/24.4.2018 (Task 7.3)

The Monday and Tuesday sessions of each week cover the same material.