ETH Zürich, D-INFK
Spring 2019

Prof. Ueli Maurer
Fabio Banfi
Daniel Jost
Jiamin Zhu

Cryptography Foundations
Solution Exercise 8

8.1 Changing the Distribution of Bit-Guessing Problems

a) Recall the solution to Exercise 1.3 a): In order to bound the distinguishing advantage $\Delta(X, X')$ we defined the set $\mathcal{X}^* := \{x \in \mathcal{X} \mid \mathsf{P}_{X'}(x) \geq \mathsf{P}_X(x)\}$ and proved that $\delta(X, X') = \Pr[X' \in \mathcal{X}^*] - \Pr[X \in \mathcal{X}^*]$. Stated differently, $\mathcal{X}$ is the set of elementary events and $\mathcal{X}^* \subseteq \mathcal{X}$ is a particular event and, and thus we can write $\delta(X, X') = \Pr^{X'}[\mathcal{X}^*] - \Pr^X[\mathcal{X}^*]$. As explained in that solution, the definition of this set follows from a maximum likelihood argument. More generally, for two probability spaces $(\Omega, \mathcal{F}, \mathsf{P}_X)$ and $(\Omega, \mathcal{F}, \mathsf{P}_{X'})$ we have that

$$\delta(X, X') = \sup_{\mathcal{B} \in \mathcal{F}} \left| \Pr^{X'}[\mathcal{B}] - \Pr^X[\mathcal{B}] \right|,$$

which is another common formulation of the statistical distance. In Exercise 1.3 a) we actually proved this for the special case in which we have the countable sample space $\Omega = \mathcal{X}$ and event set $\mathcal{F} = 2^\Omega$. This is the typical case in this lecture.

It is not hard to see that for any event $\mathcal{A} \in \mathcal{F}$ we have

$$\Pr^{X'}[\mathcal{A}] - \Pr^X[\mathcal{A}] \leq \sup_{\mathcal{B} \in \mathcal{F}} \left(\Pr^{X'}[\mathcal{B}] - \Pr^X[\mathcal{B}] \right) \leq \sup_{\mathcal{B} \in \mathcal{F}} \left| \Pr^{X'}[\mathcal{B}] - \Pr^X[\mathcal{B}] \right| = \delta(X, X').$$

b) Exercise 4.4 in the lecture notes asks to show that for a bit-guessing problem $[\![S; B]\!]$ and a distinguisher D for it, if one changes the instance distribution of (S, B) by at most d in terms of statistical distance, then the performance of D changes by at most $2d$. The performance of D is measured in terms of its advantage $\Lambda^D\big([\![S; B]\!]\big)$. Changing the instance distribution of $[\![S; B]\!]$ as described above means considering a new bit-guessing problem $[\![S'; B']\!]$ such that $d = \delta([\![S; B]\!], [\![S'; B']\!])$. We assume without loss of generality that the output bit B of S is a deterministic function of S and thus the statistical distance of $\delta([\![S; f(S)]\!], [\![S'; f(S)]\!])$ is no greater than $\delta(S, S')$ as we know from Exercise 7.3 **a)**.

In summary: what we want to prove

$$\Lambda^D\big([\![S'; B']\!]\big) \leq \Lambda^D\big([\![S; B]\!]\big) + 2 \cdot \delta(S, S').$$

Consider the random experiment $D(S, B)$, i.e., a distinguisher D interacting with system S (which outputs bit B) and outputs a guess Z, as a probability space where the elementary events correspond to sampling D and sampling S. All properties, including the event $\mathcal{A} := Z = B$ are deterministic functions when given these (sampled) problem instance and distinguisher. From subtask **a)**, we conclude that

$$\begin{aligned}
\Lambda^D\big([\![S'; B']\!]\big) - \Lambda^D\big([\![S; B]\!]\big) &= 2 \cdot \Pr^{D(S',B')}[Z' = B'] - 1 - (2 \cdot \Pr^{D(S,B)}[Z = B] - 1) \\
&= 2 \cdot (\Pr^{D(S',B')}[\mathcal{A}] - \Pr^{D(S,B)}[\mathcal{A}]) \\
&\leq 2 \cdot \delta((D, S, B), (D, S', B')) \\
&\leq 2 \cdot \delta((D, S), (D, S')) \\
&\leq 2 \cdot \delta(S, S').
\end{aligned}$$

Note that $Z = B$ and $Z' = B'$ denote the same event in the two experiments (expressed as a function of D and S)[1]. The final step that $\delta((D,S),(D,S')) \leq \delta(S,S')$ follows from a simple property of the statistical distance (analog to one of the properties proven on the previous exercise sheet) since by definition of the random experiment, D and S (resp. S') are sampled independently.

8.2 Amplifying the Performance of a Worst-Case Solver

Let X_i for $i \in \{1,\dots,q\}$ be the binary random variable that is 1 if the ith invocation of S returns the correct bit. Since S has performance ϵ, we have $p := \Pr[X_i = 1] = \frac{\epsilon}{2} + \frac{1}{2}$. Note that all X_i are independent and that the solver T outputs the wrong bit if and only if S outputs more wrong than correct bits. That is, the probability that T outputs the wrong bit is $\Pr\left[\sum_{i=1}^{q} X_i < \frac{q}{2}\right]$. Let $\alpha := \frac{\epsilon}{2} = p - \frac{1}{2}$. We then obtain for the probability that T outputs the wrong bit using Hoeffding's inequality

$$\Pr\left[\sum_{i=1}^{q} X_i < \frac{q}{2}\right] \leq \Pr\left[\sum_{i=1}^{q} X_i \leq (p-\alpha)q\right] \leq e^{-2\alpha^2 q} = e^{-q\epsilon^2/2}.$$

For $q \geq \frac{2}{\epsilon^2} \cdot \log \frac{2}{\delta}$, we have

$$e^{-q\epsilon^2/2} \leq e^{-\log(2/\delta)} = e^{\log(\delta/2)} = \frac{\delta}{2}.$$

Hence, the success probability of T for such q is at least $1 - \frac{\delta}{2}$, and the performance of T is at least $1 - \delta$.

8.3 The Next Bit Test

Recall that for an integer i the notation a^i denotes the sequence $a_1,\dots,a_i$, and that we denote its concatenation with another sequence b^j (namely, the sequence $a_1,\dots,a_i,b_1,\dots,b_j$) as $a^i\, b^j$. For this task we further introduce the following notation: for integers $i \leq j$, we write $a^{i:j}$ to denote the sequence $a_i, a_{i+1},\dots,a_j$.

In the following, let $H_k := X^k\, U^{k+1:\ell}$ for every $i \in \{1,\dots,\ell\}$, and observe that for every i can easily construct a distinguisher D_i such that

$$\Delta^D\big(H_i, H_{i-1}\big) = \Delta^{D_i}\big([X^{i-1}U^{i+1:\ell}, X_i], [X^{i-1}U^{i+1:\ell}, U_i]\big)$$

by simply inserting the bit at the i-th position and then invoking D. By Lemma 2.4, as proven in Exercise 1.3 b), we moreover know that there exists a distinguisher D_i' such that

$$\Delta^{D_i}\big([X^{i-1}U^{i+1:\ell}, X_i], [X^{i-1}U^{i+1:\ell}, U_i]\big) = \frac{1}{2}\Lambda^{D_i'}\big([\![X^{i-1}U^{i+1:\ell}; X_i]\!]\big).$$

Furthermore, it is easy to see that we can construct the predictor P_i with the same success probability as D_i' by sampling $U^{i+1:\ell}$, appending it to its input, and then invoking D_i'. Putting everything together, we obtain

$$\Delta^D\big(H_i, H_{i-1}\big) = \frac{1}{2}\Lambda^{P_i}\big([\![X^{i-1}; X_i]\!]\big).$$

Now observe that by definition $H_0 = U^\ell$ and $H_\ell = X^\ell$. Combining this with Lemma 2.2 we obtain

$$\epsilon = \Delta^D(X^\ell, U^\ell) = \Delta^D(H_\ell, H_0) = \sum_{i=1}^{\ell} \Delta^D(H_i, H_{i-1}).$$

Thus, by an averaging argument there has to exists an $i \in \{1,\dots,\ell\}$ such that $\Delta^D\big(H_i, H_{i-1}\big) \geq \frac{\epsilon}{\ell}$ and thus $\Lambda^{P_i}\big([\![X^{i-1}; X_i]\!]\big) \geq \frac{2\epsilon}{\ell}$.

[1]This means that we can identify the subset of pairs of deterministic systems from the product space $\mathcal{D} \times \mathcal{S}$ for which the output bit of the distinguisher equals the bit of the bit-guessing problem.