

Cryptography Foundations

Exercise 8

8.1 Changing the Distribution of Bit-Guessing Problems

Goal: Show that the performance of a distinguisher for a bit-guessing problem does not change much if the distribution of the problem is changed only slightly.

- a) Show that for any two random variables X and X' over some set \mathcal{X} , and any event $\mathcal{A} \subseteq \mathcal{X}$, we have

$$\Pr^X[\mathcal{A}] - \Pr^{X'}[\mathcal{A}] \leq \delta(X, X').$$

- b) State formally Exercise 4.4 from the lecture notes and prove the statement using the result from subtask a).

8.2 Amplifying the Performance of a Worst-Case Solver

Goal: Understand the bounds in Idea 4 of the reduction in the lecture notes.

Let S be a solver with performance $\epsilon > 0$ on each instance of some bit guessing problem (i.e., S has worst-case performance ϵ). Let $q \in \mathbb{N}$ be odd and let T be the solver that invokes S (each time with fresh and independent randomness) q times and then outputs the bit that was returned more often by S . Find for all $\delta \in (0, 1)$ a bound on q such that the performance of T is at least $1 - \delta$ whenever q exceeds this bound.

Hint: Use a variant of Hoeffding's inequality for Bernoulli random variables, which states the following: Let $\alpha \in (0, 1)$ and let X_1, \dots, X_q be independent and identically distributed random variables over $\{0, 1\}$ with $p := \Pr[X_i = 1]$. Then, $\Pr[\sum_{i=1}^q X_i \leq (p - \alpha)q] \leq e^{-2\alpha^2 q}$.

8.3 The Next Bit Test

Goal: When you can predict the i -th bit from the first $i - 1$ bits in a random bit-string, then you can distinguish this bit-string from the uniform string. Interestingly, the converse also holds. Therefore, unpredictable bit-strings are indistinguishable.

Let $X^\ell = (X_1, \dots, X_\ell)$ be an arbitrarily distributed random variable on the set $\{0, 1\}^\ell$, for some $\ell \geq 1$. A *predictor* of the i -th bit of X^ℓ is a distinguisher for the following bit-guessing problem: given $X^{i-1} = (X_1, \dots, X_{i-1})$, output a guess $Z \in \{0, 1\}$ for X_i . Prove that when D is a distinguisher of X^ℓ from the uniformly distributed bitstring $U^\ell = (U_1, \dots, U_\ell) \in \{0, 1\}^\ell$ with advantage ϵ , then there is an $i \in \{1, \dots, \ell\}$ and a predictor P_i of the i -th bit of X^ℓ with advantage at least $\frac{2\epsilon}{\ell}$.

Hint: You should use a result about the distinguishing advantage proven in Exercise 1.3 b).

Discussion of solutions:

23/24.4.2018 (Task 8.1 and Task 8.2)

Wednesday, 2.5.2018 (Task 8.3) **instead of the lecture**

(Note that we cancel the exercise sessions on 30.4.2018 and 1.5.2018)