Randomness in Cryptography
Homework exercise 1
Sebastian Faust

November 15, 2016

In this exercise we repeat some basic concepts from information theory and extractors. Hand-in of the exercise is Nov. 22 until 16:00 (you can give it to me after the lecture). We will discuss the solutions on Nov. 23 in the exercise session.

You need to reach 30 points to get the maximum grade for this homework assignment. In total (for all homework assignments during the semester) you can achieve up to 10 bonus points for the exam.

Exercise 1 (Statistical distance) ***(7 points)*** Prove the following properties of the statistical distance.

1. Let X, Y be binary random variables, then $\Delta(X;Y) = |\Pr[X = 1] - \Pr[Y = 1]|$. *(2 points)*
2. For all random variables X, Y, Z defined over a finite set S: $\Delta(X;Z) \leq \Delta(X;Y) + \Delta(Y;Z)$. *(2.5 points)*
3. Let X, Y, Z be random variables, where X and Z are independent, and Y and Z are independent. Then $\Delta((X,Z);(Y,Z)) = \Delta(X;Y)$. Recall that for random variables X, Y that are defined on a probability space, the joint probability distribution for X, Y is defined by $\Pr[X = a \wedge Y = b]$. The above distance is about the distance between the two joint probability distributions. *(2.5 points)*

Exercise 2 (Min-entropy) ***(5 points)***

1. Give an example of a source with min-entropy k over n bits. *(1 point)*
2. Recall the definition of Shannon entropy as $H_2(X) = -\sum_x \Pr[X = x] \log_2(\Pr[X = x])$. Given an example of a source that has high Shannon entropy but low min-entropy. *(2 points)*
3. Let $\mathbb{H}_\infty(X) \geq k$ and let Y be independent of X and uniform over $\{0,1\}^n$. Give a bound for $\mathbb{H}_\infty(X,Y)$. What happens to $\mathbb{H}_\infty(X,Y)$ if $Y = f(X)$? *(2 points)*

Exercise 3 (Extractors) ***(8 points)***

1. Suppose we have n binary sources X_i which are δ_i biased (i.e., $\Pr[X_i = 1] = \delta_i$ for some $\delta \leq \delta_i \leq 1 - \delta_i$). Assume that there is no other available source of randomness. How can we generate a single bit that is statistically close to uniform? *(1,5 points)*
2. The quality of seeded randomness extractors depends on several parameters. Explain these parameters and describe what is the goal when we design randomness extractors. *(1,5 points)*
3. Let $\mathsf{ext} : \{0,1\}^d \times \{0,1\}^n \to \{0,1\}^m$. Show that there exists no $(k-1, 0)$-seeded randomness extractor ext with $m > k + d$. *(5 points)*

Exercise 4 (Leftover Hash Lemma) ***(10 points)***

1. Suppose we have a source X with min-entropy k. Is it possible to re-use X with different random seeds $S_1, \dots S_\ell$ for $\ell \geq 2k$? In other words: Is $(S_1, \dots S_\ell, \mathsf{ext}(S_1, X), \dots, \mathsf{ext}(S_\ell, X))$ statistically close to $(U_{\ell(d+m)})$? You may think of ext being the inner product over bits. *(3 points)*

2. In class we defined the notion of universal hash functions $\mathcal{H} = \{h : \{0,1\}^n \to \{0,1\}^m\}$, which requires that over the choice of the hash function the probability that $h(x) = h(y)$ is upper bounded by 2^{-m}. One can relax the definition of the universal hash function and require that $\mathcal{H}$ is only δ-almost universal, where we require for some $\delta > 0$

$$\Pr[h(x) = h(y)] \leq \frac{1+\delta}{2^m}.$$

   Show that δ-almost universal hash functions yield strong randomness extractors via the leftover hash lemma. In particular, argue how it will affect the parameters (Note: you don't need to re-do the entire proof of the leftover hash lemma. It suffices to explain what changes in the proof and how it affects the final parameters). *(7 points)*