CS783: Theoretical Foundations of Cryptography Fall 2024

Assignment 2

August 14, 2024

Instructor: Chethan Kamath

Exercise 1 (Unpredictability vs. pseudorandomness)**.**

1. *(Lecture 4, Exercise 3) Let's start by writing down a simple reduction. Recall the definitions of pseudorandomness and next-bit unpredictability (a.k.a. unpredictability on the right) from Lecture 4. Show that if a PRG* G *is pseudorandom, then it is also next-bit unpredictable.*

2. *Recall the definition of first-bit unpredictability (a.k.a unpredictability on the left) as defined in Lecture 4: the predictor can ask for bits* $y_2, \cdots, y_i$ *(for* $i \in [1, n+1]$ *of its choice) and has to predict the first bit* y_1*.*

   (a) *Show that if a PRG* G *is pseudorandom, then it is also first-bit unpredictable.*

   (b) *Does the converse hold? That is, does first-bit unpredictability imply pseudorandomness? Come up with a proof or a counter-example.*

   (c) *Does first-bit unpredictability imply next-bit unpredictability? Come up with a proof or a counter-example.*

Exercise 2 (Hybrid argument)**.** *In this exercise, we will practice hybrid arguments. In each question, describe the hybrid worlds, and explain why consecutive worlds are indistinguishable.*

1. *Let* G *be a PRG that with expansion factor* $n+1$*. Consider the following construction of length-doubling PRG* G' *that came up during discussions in Lecture* 4*. To compute* $\mathsf{G}'(s)$*,*

   - *Set* $s_0 := s$ *and* $\ell := |s|$
   - *For each* $i \in [1, \ell]$*, compute* $s_i = \mathsf{G}(s_{i-1})$
   - *Output* s_ℓ

   Prove that G' *is a PRG using a hybrid argument. What are the advantages and disadvantages of this construction over the one in the lecture?*

2. *Recall the two-world definition of PRF from Definition* 1*, Lecture* 5*. Now consider the alternative definition, Definition* $1'$*, via the following experiment:*

   - *The distinguisher* D *is given query access to the PRF* $F_k(\cdot)$*, and it can (adaptively) make polynomially-many queries* $x_1, \cdots, x_q$ *to obtain* $F_k(x_1), \cdots, F_k(x_q)$*.*
   - *In the end,* D *issues a* challenge $x^* \notin \{x_1, \ldots, x_q\}$*: in the pseudorandom world it gets* $y^* := F_k(x^*)$ *and in the random world it gets a uniformly random value* r^* *from the co-domain of the PRF.*

F is a PRF if the behaviour of the distinguisher changes only by a negligible value in the two worlds. Using a hybrid argument, show that Definition $1'$ implies Definition 1, that is, any PRF that satisfies Definition $1'$ also satisfies Definition 1.

- *Hint: given a distinguisher in the sense of Definition 1, construct a distinguisher in the sense of Definition $1'$; note that the distinguisher in Definition $1'$ has much more flexibility.*

Exercise 3 (PRF or not)**.**

1. *For a PRF $\{F_k : \{0,1\}^n \to \{0,1\}^n\}_{k \in \{0,1\}^n}$, the "complementing" PRF defined as $F'_k(x) := \overline{F_k(x)}$ (where the overline denotes bit-string complement)?*

2. *For F as above, a second "complementing" PRF defined as $F'_k(x) := F_k(\overline{x})$?*

3. *Recall the tree-based construction of PRF from length-doubling PRF (Construction 2) we saw in Lecture 5. Recall that the value $F_k(x)$, $x \in \{0,1\}^n$, was computed by taking the key k as the seed of the root PRG, and computing the leaf output s_x. What about the "dual" construction where to compute $F_k(x)$, you use the input x as the seed of the root PRG, and then output the leaf value s_k?*

Exercise 4 (Weak PRFs)**.** *Recall that in the definition of PRFs, the distinguisher can (adaptively) query its oracle (which is either the PRF or a random function) on inputs of its choice. Let's consider a weaker notion where the distinguisher only gets to see output value on* random *input points. To be precise, $\{F_k : \{0,1\}^n \to \{0,1\}^n\}_{k \in \{0,1\}^n}$ is a weak PRF if for all PPT (oracle) distinguishers D, the following is negligible*

$$\delta(n) := \left| \Pr_{k \leftarrow \{0,1\}^n}[\mathsf{D}^{F_k(\$)}(1^n) = 0] - \Pr_{f \leftarrow \mathcal{F}_n}[\mathsf{D}^{f(\$)}(1^n) = 0] \right|.$$

Here the \$ in the oracle (instead of $(\cdot)$) denotes access to output on random *input points.*

1. *Show that if F is a PRF then it is also a weak PRF.*

2. *If F is a PRF, show that F', defined below, is a weak PRF, but not a PRF:*

$$F'_k(x) := \begin{cases} F_k(x) & \text{if } x \text{ is even} \\ F_k(x+1) & \text{otherwise} \end{cases}$$

Exercise 5 (Chosen Plaintext Attack (CPA))**.** *Recall the definition of CPA from Lecture 5 (cf. [KL14, Definition 3.21] for a formal definition). This exercise will help you understand CPA secrecy better.*

1. *Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a symmetric-key encryption (SKE) scheme with* deterministic *encryption. Show that Π cannot be CPA-secret.*

2. *Let $\Pi_1 = (\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ and $\Pi_2 = (\mathsf{Gen}_2, \mathsf{Enc}_2, \mathsf{Dec}_2)$ be two SKE schemes. We are in a situation where only one of the two schemes is CPA-secret (and we don't know which one). Construct a SKE scheme Π that is CPA-secret as long as Π_1 or Π_2 is secure. (Such a construction is called a "combiner".)*

- *Hint: it is instructive to first think about constructing such schemes against eavesdroppers.*

3. *(Easier version of Lecture 5, Exercise 4) Consider the following restriction of CPA, denoted CPA$'$, where the adversary cannot make any queries* after *the challenge. Show that, if the underlying PRF is secure, then Construction 1 from Lecture 5 is CPA$'$-secret. To make your life easier, assume that the PRF satisfies Definition* $1'$ *above.*

   - *Hint: Use the fact that in the random world in Definition* $1'$ *the challenge output is uniformly random and thus a OTP.*

References

[KL14] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography (3rd ed.)*. Chapman and Hall/CRC, 2014.