Fundamentals of Cryptography: Problem Set 4

Due Wed Oct 16 3PM

Collaboration is permitted (and encouraged); however, you must write up your own solutions and acknowledge your collaborators.

If a problem has **0pt**, it will not be graded.

Problem 0 Read Section 3.4, 3.5, 3.6 and the rest of Section 7 of "Introduction to Modern Cryptography (2nd ed)" by Katz & Lindell **or** Section 4, 5 of "A Graduate Course in Applied Cryptography" by Dan Boneh and Victor Shoup.

Problem 1 (6pt, Exercise 3.26 from KL) For any function $g : \{0,1\}^\lambda \to \{0,1\}^\lambda$, define $g^\$(\cdot)$ to be a *probabilistic* oracle, on input 1^λ it samples uniform $r \in \{0,1\}^\lambda$ and returns $(r, g(r))$. A keyed function F is called *weak PRF* if for all p.p.t. algorithms $\mathcal{D}$, there exists a negligible function negl such that:

$$\left|\Pr[\mathcal{D}^{F_k^\$(\cdot)}(1^\lambda) = 1] - \Pr[\mathcal{D}^{f^\$(\cdot)}(1^\lambda) = 1]\right| \le \text{negl}(\lambda),$$

where $k \in \{0,1\}^\lambda, f : \{0,1\}^\lambda \to \{0,1\}^\lambda$ are chosen uniformly.

Part A Prove that if F is PRF then it is weak PRF.

Part B Let F' be a PRF, define

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

Show that F is a weak PRF, but *not* a PRF.

Part C Is CTR-mode encryption using a weak PRF necessarily CPA-secure? Does it necessarily have indistinguishable encryptions in the presence of an eavesdropper? Prove your answers.

Part D Prove that Construction 3.30 (in Katz & Lindell) is CPA-secure if F is a weak PRF.

Problem 2 (6pt) A PRF $F : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$ is called a *puncturable PRF* if

- There is a p.p.t. algorithm $\mathsf{puncture}$, which takes a key, an input, and outputs a "punctured key".
- There is a p.p.t. algorithm eval, such that for any $x' \neq x$, we have $\mathsf{eval}(k_{-x}, x') = F_k(x')$, where $k_{-x} \leftarrow \mathsf{puncture}(k, x)$.

- If k, u are randomly sampled, $(k_{-x}, F_k(x))$ is indistinguishable from (k_{-x}, u).

  (More formally, consider a security game: the distinguisher $\mathcal{D}$ chooses x; the challenger samples random k, u, computes $k_{-x} \leftarrow \mathsf{puncture}(k, x)$, and sends

  - in case 0: $(k_{-x}, F_k(x))$, or
  - in case 1: (k_{-x}, u)

  to the distinguisher. We require that for any p.p.t. distinguisher $\mathcal{D}$, the distinguisher cannot tell which case it is with non-negligible advantage.)

Your task is to construct a puncturable PRF.

Remark: A puncturable PRF F is called a *private puncturable PRF* if k_{-x} does not reveal x. Until 2017, we don't know how to construct private puncturable PRF from standard assumptions.

Problem 3 (3pt, Exercise 4.8 from BS) Prove that, if $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ satisfies either of the following homomorphism properties, then F is not a PRF.

Part A $F(k, x \oplus c) = F(k, x) \oplus c$ for all $k, x, c \in \{0,1\}^n$.

Part B $F(k \oplus c, x) = F(k, x) \oplus c$ for all $k, x, c \in \{0,1\}^n$.

Part C $F(k_1 \oplus k_2, x) = F(k_1, x) \oplus F(k_2, x)$ for all $k_1, k_2, x \in \{0,1\}^n$.

Remark: In contrast to Part C, under well-received assumptions, there exist PRFs satisfying $F(k_1 +_1 k_2, x) = F(k_1, x) +_2 F(k_2, x)$, where the key space and the output space are interpreted as carefully-chosen groups, and $+_1, +_2$ are the corresponding group operations.