Fundamentals of Cryptography: Problem Set 3

Due Wed Oct 15 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 7.1, 7.2, 7.3 of "Introduction to Modern Cryptography (2nd ed)" by Katz & Lindell.

If you are curious about how to construct PRG from OWF, you may read "Pseudorandom Generators from One-Way Functions: A Simple Construction for Any Hardness" by Thomas Holenstein.

Problem 1 (0pt) Concentration Inequalities This problem recaps a few useful probability bounds. They show how random variables "concentrate" around their means. Section A of "Introduction to Modern Cryptography (2nd ed)" may help you answer this question.

Part A (Markov's Inequality) Let X be a random variable over non-negative real numbers. Prove that, for any $a > 0$,

$$\Pr[X \geq a] \leq \frac{\mathbb{E}[X]}{a}\,.$$

Part B (Chernoff Bound) Let $p \in [0,1]$ be a constant. Let $X_1, \ldots, X_n$ be random variables that are sampled independently from $\mathrm{Bern}(p)$. That is, for each $i \in \{1, \ldots, n\}$, we have $X_i \in \{0,1\}$ and $\Pr[X_i = 1] = p$.

(1) Compute $\mathbb{E}[e^{t\sum_i X_i}]$ for any $t \in \mathbb{R}$.

(2) Prove that,

$$\Pr\Big[\frac{1}{n}\sum_i X_i \geq p + \varepsilon\Big] \leq \frac{\mathbb{E}[e^{t\sum_i X_i}]}{e^{tn(p+\varepsilon)}}\,,$$

for any $t > 0$.

(3) Optimize the above bound by choosing t wisely.

The optimized bound is call *Chernoff bound*, it should looks like

$$\Pr\Big[\frac{1}{n}\sum_i X_i \geq p + \varepsilon\Big] \leq e^{-D(p+\varepsilon\|p)\cdot n}\,,$$

where $D(p+\varepsilon\|p)$ is the notatino of KL divergence, and is defined as $D(p+\varepsilon\|p) := (p+\varepsilon)\log(\frac{p+\varepsilon}{p}) + (1-p-\varepsilon)\log(\frac{1-p-\varepsilon}{1-p})$. Since $D(p+\varepsilon\|p) \geq 2\varepsilon^2$, *Chernoff bound* can be relaxed to

$$\Pr\Big[\frac{1}{n}\sum_i X_i \geq p + \varepsilon\Big] \leq e^{-2\varepsilon^2 n}\,.$$

Part C (Chebyshev's Inequality) Let X be a random variable. Prove that

$$\Pr\Big[|X - \mathbb{E}[X]| \geq a\Big] \leq \frac{\mathrm{Var}[X]}{a^2}$$

for any $a > 0$. Here $\mathrm{Var}[X] := \mathbb{E}[(X - \mathbb{E}[X])^2]$ is the variance of X.

Let $X_1, \ldots, X_n$ be random variables such that $\mathbb{E}[X_i] = p$ and $\mathrm{Var}[X_i] = \sigma^2$ for all i. We also assume that $X_1, \ldots, X_n$ are *pair-wise independent*. Prove that

$$\Pr\Big[\Big|\frac{1}{n}\sum_i X_i - p\Big| \geq a\Big] \leq \frac{\sigma^2}{na^2}$$

for any $a > 0$.

Problem 2 (14pt) Assume f is a length-preserving OWF (i.e., $|f(x)| = |x|$). In each of the following cases, prove f' is a OWF, or show a counterexample.

Part A $f'(x) := f(x) \| f(f(x))$.

Part B $f'(x) := x \oplus f(x)$.

Part C $f'(x) := f(x) \| f(\bar{x})$, where $\bar{x}$ denote the bit-wise NOT operation.

Part D $f'(x) := f(G(x))$, where G is a PRG that $|G(s)| = |s| + 1$.

Part E $f'(x) := G(f(x))$, where G is a PRG that $|G(s)| = |s| + 1$.

Part F $f'(x) := f(x \| \underbrace{0 \ldots 0}_{\log n \text{ many}})$, where $n = |x|$.

Part G $f'(x) := (f(x))_{1:(n-\log n)}$, where $n = |x|$. That is, $f'(x)$ outputs the first $n - \log(n)$ bits of $f(x)$.

Problem 3 (6pt) Hardness Amplification of Weak OWFs For simplicity, we consider length-preserving weak OWF. $f : \{0,1\}^* \to \{0,1\}^*$ is a length-preserving weak OWF, if $|f(x)| = |x|$ for any $x \in \{0,1\}^*$, and there exists a polynomial q, such that for any PPT $\mathcal{A}$, for any sufficiently large n,

$$\Pr_{\substack{x \xleftarrow{\$} \{0,1\}^n \\ \hat{x} \leftarrow \mathcal{A}(f(x))}}\Big[f(\hat{x}) = f(x)\Big] \leq 1 - \frac{1}{q(n)}.$$

(Note the order of the quantifiers!)

Assume f is such a weak OWF. Define f' such that for $x_1, \ldots, x_m \in \{0,1\}^n$,

$$f'(x_1 \| \ldots \| x_m) = f(x_1) \| \ldots \| f(x_m)$$

where $m = m(n)$ is a polynomial on n. ($m(n)$ will be fixed later.)

We prove f' is a OWF by contradiction. Assume f' is not a OWF, then there exists PPT $\mathcal{A}'$, and polynomial p such that

$$\Pr_{\substack{x_1, \ldots, x_m \xleftarrow{\$} \{0,1\}^n \\ \hat{x}_1, \ldots, \hat{x}_m \leftarrow \mathcal{A}'(f(x_1)\|\ldots\|f(x_m))}}\Big[f(\hat{x}_1) = f(x_1), \ldots, f(\hat{x}_m) = f(x_m)\Big] > \frac{1}{p(n)}$$

for infinitely many integer n.

Define $\mathcal{A}$ as

$$\begin{array}{ll} \mathcal{A}(y) & \text{let } n = |y|, \text{ let } m = m(n) \\ & \text{sample } i \xleftarrow{\$} \{1, \ldots, m\} \\ & \text{for all } j \neq i, \text{ sample } x_j \xleftarrow{\$} \{0,1\}^n \text{ and let } y_j = f(x_j) \\ & \text{let } y_i = y \\ & \text{call } \hat{x}_1 \| \ldots \| \hat{x}_m \leftarrow \mathcal{A}'(y_1 \| \ldots \| y_m) \\ & \text{if } f'(\hat{x}_1 \| \ldots \| \hat{x}_m) = y_1 \| \ldots \| y_m, \\ & \qquad \text{output } \hat{x}_i \end{array}$$

We say $x \in \{0,1\}^n$ is "good" if $\mathcal{A}$ inverts $f(x)$ with a good probability. Concretely, we define $x \in \{0,1\}^n$ is "good" if and only if

$$\Pr_{\hat{x} \leftarrow \mathcal{A}(f(x))} \Big[f(\hat{x}) = f(x) \Big] \geq \frac{1}{r(n)}$$

for a polynomial $r(n)$. ($r(n)$ will be fixed later.) If x is not "good", we say x is "bad".

Part A Prove that

$$\Pr_{\substack{x_1, \ldots, x_m \xleftarrow{\$} \{0,1\}^n \\ \hat{x}_1, \ldots, \hat{x}_m \leftarrow \mathcal{A}'(f(x_1) \| \ldots \| f(x_m))}} \Big[f(\hat{x}_1) = f(x_1), \ldots, f(\hat{x}_m) = f(x_m) \Big]$$
$$\leq \frac{m^2}{r(n)} + \Big(\Pr_{x \leftarrow \{0,1\}^n} [x \text{ is "good"}] \Big)^m,$$

for any sufficiently large n.

Part B Choose polynomials $m(n)$, $r(n)$ properly, so that

$$\Pr_{x \leftarrow \{0,1\}^n} [x \text{ is "bad"}] \leq \frac{1}{2q(n)}$$

for infinitely many n. (Note that, you can let $r(n)$ depend on both $p(n)$ and $q(n)$; while $m(n)$ can depend on $q(n)$ and cannot depend on $p(n)$.)

Part C Define $\mathcal{A}_{\text{repeat}}$ as

$$\begin{array}{ll} \mathcal{A}_{\text{repeat}}(y) & \text{let } n = |y| \\ & \text{repeat the following for } n \cdot r(n) \text{ times} \\ & \qquad \text{call } \hat{x} \leftarrow \mathcal{A}(y) \\ & \qquad \text{if } f(\hat{x}) = y, \\ & \qquad\qquad \text{output } \hat{x} \end{array}$$

Show that $\mathcal{A}_{\text{repeat}}$ violates our assumptions on f.

The contradiction rules out our assumption. So f' must be a OWF.

Problem 4 (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 didn't know how to construct private puncturable PRF from standard assumptions.

Problem 5 (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.