CS 6222-Cryptography, Homework 4

Response by: Your Name, (computing id)

Total points: 30. Points are noted after each problem.

Directions. For each problem, typeset your solution in the `answer` environment, and if there are sub-problems, mark them clearly. Feel free to use as much space as you want to. Before you submit the PDF, update 1) "Your Name" and id on the above, and 2) the "Acknowledgement" box at the last page properly.

Policies. We re-iterate our policy. It is encouraged to think and discuss the problems before looking for ready-made solutions. You shall acknowledge and/or reference any discussion and published material except for lecture notes and resources of LaTeX. In any case, it is a violation if any of the following cases happens:

- You copied text directly (from any source).
- You used any material or discussion without acknowledgement or citation.
- You are unable to explain your work orally.

This homework reviews the reduction from OWFs to PRG. Particularly, the problems aim to clarify some calculation and to fix a bug in the lectures.

Problem 1 (Shannon entropy, 2pt each)**.** Let X, Y be finite discrete random variables. Recall that Shannon entropy is defined to be

$$H(X) := \sum_x \Pr[X = x] \cdot \log \frac{1}{\Pr[X = x]},$$

which is the average amount of information obtained by observing (the value of) X. The *conditional* Shannon entropy is defined to be

$$H(Y|X) := \sum_{x,y} \Pr[Y = y \cap X = x] \cdot \log \frac{1}{\Pr[Y = y|X = x]},$$

which is the average amount of information obtained by observing (the value of) Y after X is known. (Both definitions follow the convention that $0 \cdot \log(1/0) = 0$.)

(a) Suppose that X and Y are independent. Prove that $H(Y|X) = H(Y)$.

(b) Prove that $H(XY) = H(Y|X) + H(X)$ for (possibly) dependent (X, Y), where XY denotes the concatenated random variable of X and Y.

(c) For any function f, prove that $H(f(X)|X) = 0$. (Notice that means, for any $Y = f(X)$ that is determined by X, $H(Y|X) = 0$.)

(d) Give a function $f : \{0,1\}^n \to \{0,1\}^n$ such that $H(X|f(X)) = 10$.

Answer.

(a)

(b)

(c)

(d)

□

Problem 2 (From PEG to PRG, 2pt each)**.** Let $G : \{0,1\}^n \to \{0,1\}^m$ be a function for some $m := m(n)$ and for all $n \in \mathbb{N}$. Assume that there exists $k := k(n)$ and an ensemble of distributions $\{Y_n\}_{n\in\mathbb{N}}$ such that all of the following hold:

- for all $n \in \mathbb{N}$ and for every $x \in \{0,1\}^n$, the cardinality of the pre-image $|G^{-1}(G(x))| = 2^k$ (so that G is 2^k-to-one),
- $H_\infty(Y_n) \geq n - k + n^{0.1}$, and
- $\{Y_n\}_{n\in\mathbb{N}} \approx_c \{G(U_n)\}_{n\in\mathbb{N}}$ (where Y_n is a variable over $m(n)$-bit strings).

For all $n \in \mathbb{N}$ and $x \in \{0,1\}^n$, define

$$g(x, M_1, M_2) := M_1 \| M_2 \| M_1 \odot G(x) \| M_2 \odot x,$$

where $M_1 \in \{0,1\}^{\ell_1 \times m}, M_2 \in \{0,1\}^{\ell_2 \times n}$, and $\ell_1 := n - k + n^{0.1}/2$ and $\ell_2 := k - n^{0.1}/2 + 1$. Also suppose that $\ell_1, \ell_2 > 0$.

(a) Calculate the input length and output length of g in terms of n, m, and k.

(b) Let $x \leftarrow \{0,1\}^n$ be uniformly sampled at random. Calculate $H_\infty(x)$ given the value $G(x)$ using the definition of min-entropy [Vad12, Definition 6.7].

(c) Calculate (an upper bound of) the statistical difference [Vad12, Definition 6.2] between the two distributions $D_0 := (M_1 \| M_2 \| M_1 \odot G(x) \| M_2 \odot x)$ and $D_1 := (M_1 \| M_2 \| M_1 \odot G(x) \| U_{\ell_2})$ using Leftover Hash Lemma [Vad12, Theorem 6.18], where variables (x, M_1, M_2) are uniformly sampled from the input domain of G, and U_ℓ is an independently and uniformly sampled ℓ-bit string for all ℓ.

(d) Are the two distributions D_1 and $D_2 := (M_1 \| M_2 \| M_1 \odot Y_n \| U_{\ell_2})$ computationally indistinguishable? Write a proof by reduction.

(e) Calculate (an upper bound of) the statistical difference between the two distributions D_2 and $D_3 := (M_1 \| M_2 \| U_{\ell_1} \| U_{\ell_2})$ using Leftover Hash Lemma.

(f) Put together all above items and conclude that g is a PRG by Hybrid Lemma.

(g) Does the ordering of hybrids D_0, D_1, D_2, D_3 matter? That is, can we alternatively define $D_1' := (M_1 \| M_2 \| M_1 \odot Y_n \| M_2 \odot x)$ and argue that D_0 and D_1' are computationally indistinguishable?

Answer.

(a)

(b)

(c)

(d)

(e)

(f)

(g)

□

Problem 3 (Weak PRGs, 3,3,2pt)**.** Let $g_1, g_2 : \{0,1\}^n \to \{0,1\}^{n+1}$ be two functions for all n. Suppose that at least one of the two functions is a PRG (but we do not know which).

(a) In a previous lecture, the instructor (Wei-Kai) said that $g(x) := g_1(x) \oplus g_2(x)$ is a PRG. Is g indeed a PRG? Justify your answer.

(b) Consider another $g(x_1, x_2) := g_1(x_1) \oplus g_2(x_2)$. Is g a PRG (that is, expanding and pseudorandom)?

(c) How to obtain a PRG from g_1 and g_2? Suggest a candidate construction and briefly explain why your construction is a secure PRG. (Hint: we showed extending from $(n+1)$-bit PRG to $2n$-bit PRG.)

Answer.

(a)

(b)

(c)

□

Acknowledgement

Replace this with your collaborators and resources like below (if you did not have any, replace this with *None*).

Problem 1 is inspired by a discussion with Jonathan, who explained Extended Euclidean Algorithm to me.

Problem 2: I used ChatGPT with the prompt "teach me DMT2" and obtained XXX.

Problem 3: Step X is followed by [KL21, Theorem Y, page Z].

References

[KL21] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. CRC Press, Massachusetts, 3 edition, 2021.

[Vad12] Salil P. Vadhan. *Pseudorandomness*. Foundations and Trends in Theoretical Computer Science, 2012. https://people.seas.harvard.edu/~salil/pseudorandomness/pseudorandomness-published-Dec12.pdf.