CS6222 Grad Cryptography, Homework 2

Response by: Your Name, (Computing ID)

Total points: 35 awarded maximum. 44 available. Points are noted after each problem.

Instructions. 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 require, and be sure to update your name and computing ID above, and the acknowledgements box at the end.

Policies. In short, you are encouraged to think about the problems on your own, and then discuss them and work toward solutions with your classmates. You must write and submit your own solutions. You may also read any published material that helps you come to an understanding of the problems, but you must acknowledge and/or reference any discussion or published material, with the exception of lecture notes, in-class and in-office-hours discussions, textbook sections we have covered, and basic LaTeX help or dictionary lookups. It is a violation of the honor code if any of the following occur:

- You copy text directly from any source.
- You use any material or discussion without acknowledgment or citation, excluding the above special cases.
- You are unable to explain your work orally.

See https://jackdoerner.net/teaching/2025/Fall/CS6222/#policies for more details.

Problem 1 (PRG or Not?, 3pts each)**.** Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG. For each of these sub-problems you must determine whether the proposed constructions of G' are *necessarily* PRGs or not. Justify your answer by providing either a short proof (if G' *must be* a PRG), or disproof (if it *might not be*). A disproof consists of an algorithm that distinguishes the output of G' from a uniform string with non-negligible probability. In some cases, it might be possible to write a distinguisher that works for *any* PRG G, but in others, you may need to write a distinguisher that works only for some *specific* G. In the latter cases, provide a description of that specific G and a short proof that it is a PRG. If necessary, you can assume there exists some other PRG G'' and then use G'' to construct the specific G you require.

(a) $G' : s \mapsto G(s\|0)$

(b) $G' : s \mapsto G((s+1) \bmod 2^{|s|})$ (i.e. interpret s as an $|s|$-bit integer, and add 1 modularly)

(c) $G' : s \mapsto G(s)\|G((s+1) \bmod 2^{|s|})$

(d) $G' : s \mapsto G(s) \oplus (0^n\|s)$

Problem 2 (Combining PRGs (5pts))**.** Suppose there are two *candidate* PRGs, $G_1 : \{0,1\}^n \to \{0,1\}^{n+1}$ and $G_2 : \{0,1\}^n \to \{0,1\}^{n+1}$. Some people believe that only G_1 is a PRG, and some people believe that only G_2 is a PRG. Make everybody happy by constructing a single PRG G' and proving that G' is secure if at least one of G_1 and G_2 is secure.

Problem 3 (PRF or Not?, 3pts each)**.** Let $\{F_k : \{0,1\}^{|k|} \to \{0,1\}^{|k|}\}_{k\in\{0,1\}^*}$ be a PRF family. For each of these sub-problems you must determine whether the proposed constructions of F'_k are *necessarily* PRFs or not. Justify your answer by providing either a short proof (if F'_k *must be* a PRF), or a disproof (if it *might not be*). Note that some of the constructions have different input or output lengths from F_k; we care that each candidate is oracle-indistinguishable from a random function with a domain and codomain that match the candidate. As in Problem 1, a disproof requires a distinguisher algorithm, which might work only for some specific F_k that you specify. You may assume the existence of additional PRFs with different input or output lengths in order to construct a specific F_k, if necessary.

(a) $F'_k : x \mapsto F_k(x\|0)\|F_k(x\|1)$

(b) $F'_k : x \mapsto F_k(0\|x)\|F_k(x\|1)$

(c) $F'_k : x \mapsto F_k(x) \oplus x$

(d) $F'_k : x \mapsto F_x(k)$

Problem 4 (PRF Expansion via PRG (5pts))**.** In class, the instructor asserted that if $\{F_k : \{0,1\}^{|k|} \to \{0,1\}^{|k|}\}_{k\in\{0,1\}^*}$ is a PRF family and $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ is a PRG, then

$$F'_k : x \mapsto G(F_k(x))$$

also defines a PRF family, with $\ell(n)$-bit outputs. Prove that this is true.

Hint: you may need to define a hybrid experiment, but you should need one hybrid at most. Your proof must use both assumptions: that both F and G are secure.

Problem 5 (CPA-Insecure Encryption (10pts))**.** In class we defined the Multi-Message Eavesdropping game[1] $\mathsf{EAV}_b^{\Pi,\mathcal{A}}(n)$ for a symmetric-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ and a two-part adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$:

1. $k \leftarrow \mathsf{Gen}(1^n)$
2. $(\vec{m}^0, \vec{m}^1, s) \leftarrow \mathcal{A}_1(1^n)$ such that $|\vec{m}^0| = |\vec{m}^1|$ and $|m_i^0| = |m_i^1| = n$ for every $i \in [t]$, where $(m_1^b, \ldots, m_t^b) = \vec{m}^b$ for $b \in \{0,1\}$
3. $c_i \leftarrow \mathsf{Enc}_k(m_i^b)$ for every $i \in [t]$
4. Output $\mathcal{A}_2(s, (c_1, \ldots, c_t))$

Additionally, we defined the Chosen Plaintext Attack Indistinguishiability game[2] $\mathsf{INDCPA}_b^{\Pi,\mathcal{A}}(n)$:

1. $k \leftarrow \mathsf{Gen}(1^n)$
2. $(m^0, m^1, s) \leftarrow \mathcal{A}_1^{\mathsf{Enc}_k(\cdot)}(1^n)$ such that $|m^0| = |m^1| = n$
3. $c \leftarrow \mathsf{Enc}_k(m^b)$
4. Output $\mathcal{A}_2^{\mathsf{Enc}_k(\cdot)}(s, c)$

[1] The version we gave in class allowed messages to be of *any* length, but in order to make this problem simpler, I have modified the game to fix the message length to be n bits.

[2] As above, I have modified the game to fix the length of all messages to be n bits, for simplicity.

We said that an encryption scheme Π is EAV-secure if for every NUPPT $\mathcal{A}$ there exists some negligible function ε such that $\forall n \in \mathbb{N}$,

$$\left| \Pr\left[\mathsf{EAV}_b^{\Pi,\mathcal{A}}(n) = b : b \leftarrow \{0,1\} \right] - \frac{1}{2} \right| < \varepsilon(n)$$

and that Π is INDCPA-secure if

$$\left| \Pr\left[\mathsf{INDCPA}_b^{\Pi,\mathcal{A}}(n) = b : b \leftarrow \{0,1\} \right] - \frac{1}{2} \right| < \varepsilon(n)$$

Assuming the existence of a pseudorandom function family, design an encryption scheme that is EAV secure, but *not* CPA secure. That is, you should provide both a proof of EAV security for your scheme, and an attack against its INDCPA security.

Hint: Your encryption scheme does not need to be *natural*. The main difference between the two games is that the adversary can adaptively request encryptions of messages that depend upon previous ciphertexts in the INDCPA game. How can you leverage this to make your scheme fail?

Acknowledgments

In this box, you should acknowledge your collaborators and the resources you used, if any. For example:

Problem 1: I discussed this problem with Alice and Bob. In addition, I asked Carol for help understanding Conditional Probability, but we did not discuss the problem further.

Problem 2: I asked ChatGPT "What is a turing machine?", and it gave me the following transcript: https://chatgpt.com/share/68b4dba7-e19c-8013-a137-e8db901493b7.

Problem 3: It helped me to read the proof of [Vad12, Theorem X, Page Y].

Instructor's Acknowledgments

Problems in this homework have been borrowed from or inspired by a number of sources. Citations can be provided on request, after the homework is completed.

References

[Vad12] Salil P. Vadhan. *Pseudorandomness*. 2012. https://people.seas.harvard.edu/~salil/pseudorandomness/pseudorandomness-published-Dec12.pdf.