UC Berkeley — CS171 : Undergraduate Cryptography
Prof. Sanjam Garg

Midterm I
September 22, 2021

Midterm I

Name:

SID:

- **Try to answer all questions. Not all parts of a problem are weighted equally. Before you answer any question, read the problem carefully. Be precise and concise in your answers.**
- **You may consult at most *10 sheets of notes*. Apart from that, you may not look at books, notes, etc. Calculators, phones, computers, and other electronic devices are NOT permitted for looking up content. However, you may use an electronic device such as a tablet for writing your answers.**
- **You have 80 minutes: there are 5 questions on this exam worth a total of 100 points.**
- **You are allocated 90 minutes and the extra 10 minutes are provided for the submission of the exam on Gradescope. You must submit/upload the exam on time. Note that late submissions will not be accepted.**
- **DSP Students must submit the exam in time as per your accommodation. Thus, if you are allowed $1.5\times$ (resp., $2\times$) the exam time then you must submit it within $80 * 1.5 + 10$ (resp., $80 * 2 + 10$) mins, i.e. 130 (resp., 170) mins. Please make your submission via email to both sanjamg@berkeley.edu and yinuo@berkeley.edu using the subject “CS 171: Midterm 1 DSP Submission.”**
- **The exam must be submitted before 8 PM PT on Feb 22nd, 2021. No exams later than this time will be accepted regardless of when you start the test.**
- **We will not be answering questions during the exam. If you feel that something is unclear please write a note in your answer.**

Name: □

1 True/False (20 points)

Bubble in the right answer. No explanation needed. +2 points for correct answer and ***-1 points for wrong answers!*** *If you leave a question unanswered, then there is no penalty. This part will be graded automatically. Please mark your answer clearly.*

1. Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function. Then, $f'_k(x,y) = f_k(x) \| x \oplus f_k(y)$ is a pseudorandom function.

   ○ True

   ○ False

   Solution: False

2. $$f(n) = \begin{cases} 2^{-\log^2 n} & n \text{ is odd} \\ 2^{-n} & n \text{ is even} \end{cases}$$

   is a non-negligible function.

   ○ True

   ○ False

   Solution: False

3. Consider an encryption scheme where ciphertexts contain no information about the secret key. Then, the scheme must be CPA-secure.

   ○ True

   ○ False

   Solution: False

4. A mult-secure encryption scheme is also CPA-secure.

   ○ True

   ○ False

   Solution: False

5. Consider a variant of the mult security definition called mult-(+1) where the adversary is additionally allowed a single phase-2 encryption query. Any encryption scheme that is mult secure is also mult-(+1) secure.

○ True

○ False

Solution: False

6. The number of permutations from $\{0,1\}^n$ to $\{0,1\}^n$ is $(2^n)!$.

   ○ True

   ○ False

   Solution: True

7. There exists a perfectly secure encryption scheme such that $\mathsf{Enc}(k,m) = m$ with non-zero probability.

   ○ True

   ○ False

   Solution: True

8. Let $g : \{0,1\}^\ell \to \{0,1\}^m, f : \{0,1\}^m \to \{0,1\}^n$ be two functions such that one of them is a pseudorandom generator. Then, $f(g(\cdot))$ is a pseudorandom generator.

   ○ True

   ○ False

   Solution: False

9. Let $g_k : \{0,1\}^\ell \to \{0,1\}^\ell, f_s : \{0,1\}^\ell \to \{0,1\}^\ell$ be two functions such that one of them is a pseudorandom function and the other one is a permutation (i.e., a bijective function). Then, $f_s(g_k(\cdot))$ is a pseudorandom function.

   ○ True

   ○ False

   Solution: True

10. Let $g_k : \{0,1\}^\ell \to \{0,1\}^m$ be a pseudorandom function and $f : \{0,1\}^m \to \{0,1\}^n$ be a pseudorandom generator. Then, $f(g_k(\cdot))$ is a pseudorandom function.

    ○ True

    ○ False

    Solution: True

2 Pseudorandom Generators (25 points)

Let $g : \{0,1\}^n \to \{0,1\}^{n+1}$ be a psuedorandom generator with stretch 1 (that is, its output is 1 bit longer than its seed). We will show how to construct from g a PRG $f : \{0,1\}^n \to \{0,1\}^{n+2}$ with stretch 2. First, we will show an insecure attempt at expanding the stretch, and then you will be asked to demonstrate a secure method of expanding the stretch.

1. Consider the following attempt at defining f. On input seed $s \in \{0,1\}^n$, f computes $t \coloneqq g(s)$ and then outputs $(t_1, g(t_{1,\dots,n})) \in \{0,1\}^{n+2}$, where t_1 is the first bit of t, and $t_{1\dots,n}$ are the first n bits of t. We will construct a PRG g for which f as defined above is **not** a PRG.

   (a) Using a PRG $h : \{0,1\}^{n-1} \to \{0,1\}^n$, construct a $g : \{0,1\}^n \to \{0,1\}^{n+1}$ for which f as defined above is not secure. Below, write a description of g, and argue that the resulting f is not a secure PRG. (5 points)

   Solution: On input seed $s \in \{0,1\}^n$, g outputs $(s_1, h(s_{2,\dots,n}))$. The first two output bits of f will always be equal.

   (b) Prove that the g you specified above is a secure PRG, assuming that h is a secure PRG. (5 points)

   Solution: The reduction pre-pends a uniformly random bit s_1 to the challenger's output.

2. Now, assuming that $g : \{0,1\}^n \to \{0,1\}^{n+1}$ is a PRG, define and prove the security of a PRG $f : \{0,1\}^n \to \{0,1\}^{n+2}$. (15 points)

   Solution: On input seed $s \in \{0,1\}^n$, f computes $t \coloneqq g(s)$ and then outputs $(t_1, g(t_{2,\dots,n+1}))$. Define a hybrid where t is replaced with u for random $u \leftarrow \{0,1\}^{n-1}$.

3 CPA Security (20 points)

Consider the following variants of CPA security. Weak-1-CPA is the same as CPA security, except that the adversary is only allowed exactly 1 phase-1 query. Weak-2-CPA is the same as CPA security, except that the adversary is only allowed exactly 2 phase-1 queries. Assuming the existence of a CPA-secure scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, construct a scheme $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ that provably satisfies Weak-1-CPA security but does **not** satisfy Weak-2-CPA security,

1. Define your scheme $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ and argue that it does not satisfy Weak-2-CPA security. (10 points)

   Solution:

   - $\mathsf{Gen}'(1^\lambda)$: Sample $k \leftarrow \mathsf{Gen}(1^\lambda)$ and $r_0, r_1 \leftarrow \{0,1\}^\lambda$
   - $\mathsf{Enc}'((k, r_0, r_1), m)$: If $m = r_0 \oplus r_1$ output m, otherwise sample $b \leftarrow \{0,1\}$ and output $\mathsf{Enc}(k, m), r_b$.
   - Decryption is straightforward

   This does not satisfy Weak-2-CPA since an adversary can query for any two arbitrary encryptions and learn both r_0, r_1 with probability 1/2. In this case it can include $m^* = r_0 \oplus r_1$ as one of its challenge ciphertexts.

2. Prove that your scheme satisfies Weak-1-CPA security. (10 points) **Solution:** Reduction samples $r_0, r_1 \leftarrow \{0,1\}^\lambda$. Prove that i) with 1 phase-1 query probability of guessing $m^* = r_0 \oplus r_1$ is negligible, and ii) if the adversary does not query m^* as one of its challenges, the reduction succeeds.

Name:

4 Double Encryption (20 points)

1. Give an example of an $\mathsf{PrivK}^{\mathsf{eav}}$ secure scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ such that the scheme $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ is **not** $\mathsf{PrivK}^{\mathsf{eav}}$ secure, where $\mathsf{Gen}' = \mathsf{Gen}$, $\mathsf{Enc}'(k, m) = \mathsf{Enc}(k, \mathsf{Enc}(k, m))$, and $\mathsf{Dec}'(k, c) = \mathsf{Dec}(k, \mathsf{Dec}(k, c))$. (10 points) **Solution:** Psuedo-OTP: $\mathsf{Enc}(k, m) = G(k) \oplus m$. $\mathsf{Enc}(k, \mathsf{Enc}(k, m))) = G(k) \oplus G(k) \oplus m = m$.

2. Prove that for any CPA-secure scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, the scheme $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ where $\mathsf{Gen}' = \mathsf{Gen}$, $\mathsf{Enc}'(k, m) = \mathsf{Enc}(k, \mathsf{Enc}(k, m))$, and $\mathsf{Dec}'(k, c) = \mathsf{Dec}(k, \mathsf{Dec}(k, c))$ is also CPA-secure. (10 points) **Solution:** Reduction will re-encrypt each ciphertext using its encryption oracle.

5 Fill in the Blanks (15 points)

1. How many functions are there from $\log_2(n)$ bits to n^2 bits? (5 points)

   Solution: n^3

2. Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a CPA-secure encryption scheme. Construct a CPA-secure encryption scheme Π' that is **not** CCA-secure. Do not use any other crytographic primitives (e.g. PRG,PRF) in your construction. Provide a brief explanation for why the scheme is not CCA-secure. (5 points)

   Solution: Encryption samples $b \leftarrow \{0,1\}$ and outputs $\mathsf{Enc}(k,m), b$. The attacker can flip the final bit of its challenge ciphertext and submit it to the decryption oracle to learn what message was encrypted.

3. Show that CBC mode encryption is not CCA-secure. (5 points)

   Solution: Given their challenge ciphertext $\mathsf{Enc}(k, m_b)$, attacker can flip a bit of the initialization vector and submit the ciphertext to the decryption oracle to learn $m_b \oplus 1$.