

Assignment 1

Perfect Security, PRGs

Instructor: Sruthi Sekar

Problem 1 (Alternate Definition of Perfect Secrecy?). Prove or refute: An encryption scheme with message space $\mathcal{M}$ is perfectly secret if and only if every probability distribution over $\mathcal{M}$ and every $c_0, c_1 \in \mathcal{C}$ we have $\mathbb{P}[C = c_0] = \mathbb{P}[C = c_1]$.

Problem 2 (Bounds for Perfect Indistinguishability). Prove that a scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ satisfying perfect indistinguishability [Definition 4, Lecture 2] must have $|\mathcal{K}| \geq |\mathcal{M}|$ without using the equivalence of the different perfect security definitions. Recall that we used perfect security [Definition 2, Lecture 2] to prove this in [Theorem 2, Lecture 2]. Specifically, for an arbitrary encryption scheme Π with $|\mathcal{K}| < |\mathcal{M}|$, show an adversary Eve for which $\mathbb{P}[\text{Priv}_{\text{Eve}, \Pi} = 1] > \frac{1}{2}$ (refer to [Definition 4, Lecture 2] for $\text{Priv}_{\text{Eve}, \Pi}$).
(Hint: Use the power of Eve being randomized.)

Problem 3 (Correctness with Errors). Assume we require only that an encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ with message space $\mathcal{M}$ satisfy the following: For all $m \in \mathcal{M}$, we have $\mathbb{P}[\text{Dec}(k, \text{Enc}(k, m)) = m] \geq 2^{-t}$. (This probability is taken over the choice of the key as well as any randomness used during encryption.) Show that perfect secrecy can be achieved with $|\mathcal{K}| < |\mathcal{M}|$ when $t \geq 1$. Prove a lower bound on the size of $\mathcal{K}$ in terms of t .

Problem 4 (Perfect Secrecy over Product Distributions). In this problem, we consider definitions of perfect secrecy for the encryption of two messages (using the same key). Here we consider distributions over pairs of messages from the message space $\mathcal{M}$; we let M_1, M_2 be random variables denoting the first and second message, respectively. (We stress that these random variables are not assumed to be independent.) We generate a (single) key k , sample a pair of messages (m_1, m_2) according to the given distribution, and then compute ciphertexts $c_1 \leftarrow \text{Enc}_k(m_1)$ and $c_2 \leftarrow \text{Enc}_k(m_2)$; this induces a distribution over pairs of ciphertexts and we let C_1, C_2 be the corresponding random variables.

- a) Say encryption scheme $(\text{Gen}, \text{Enc}, \text{Dec})$ is *perfectly secret for two messages* if for all distributions over $\mathcal{M} \times \mathcal{M}$, all $m_1, m_2 \in \mathcal{M}$, and all ciphertexts $c_1, c_2 \in \mathcal{C}$ with $\mathbb{P}[C_1 = c_1 \wedge C_2 = c_2] > 0$:

$$\mathbb{P}[M_1 = m_1 \wedge M_2 = m_2 \mid C_1 = c_1 \wedge C_2 = c_2] = \mathbb{P}[M_1 = m_1 \wedge M_2 = m_2].$$

Prove that no encryption scheme can satisfy this definition.

Hint: Take $c_1 = c_2$.

- b) Say encryption scheme $(\text{Gen}, \text{Enc}, \text{Dec})$ is *perfectly secret for two distinct messages* if for all distributions over $\mathcal{M} \times \mathcal{M}$ where the first and second messages are guaranteed to be different (i.e., distributions over pairs of distinct messages), all $m_1, m_2 \in \mathcal{M}$, and all $c_1, c_2 \in \mathcal{C}$ with $\mathbb{P}[C_1 = c_1 \wedge C_2 = c_2] > 0$:

$$\mathbb{P}[M_1 = m_1 \wedge M_2 = m_2 \mid C_1 = c_1 \wedge C_2 = c_2] = \mathbb{P}[M_1 = m_1 \wedge M_2 = m_2].$$

Show an encryption scheme that provably satisfies this definition.

Hint: The encryption scheme you propose need not be efficient, although an efficient solution is possible.

Problem 5 (BPP). *Optional HW, in case you want to understand the amplification discussion better. It will help you understand application of basic probability bounds like Chebyshev and Chernoff a little better.*

- a) Recall [Definition 5, Lecture 3] for the complexity class BPP. Prove that $L \in \text{BPP}$ (according to Definition 5), if there exists a positive polynomial $p(\cdot)$ and a randomized Turing machine M such that

- i) For every $x \in L$, it holds that $\Pr[M(x) = 1] \geq \frac{1}{2} + \frac{1}{p(|x|)}$, and
- ii) For every $x \notin L$, it holds that $\Pr[M(x) = 0] \geq \frac{1}{2} + \frac{1}{p(|x|)}$.

Hint: Given a probabilistic polynomial time machine M satisfying the above two conditions, construct an M' by running multiple copies of M (figure out how many copies) and output the majority. Use Chebyshev's inequality (refer to these [slides](#) or these [notes](#) for Chebyshev).

- b) Prove that for every $L \in \text{BPP}$ [Definition 5, Lecture 3] and every $p(\cdot)$, there exists a randomized Turing machine M such that

- i) For every $x \in L$, it holds that $\Pr[M(x) = 1] \geq 1 - 2^{-p(|x|)}$, and
- ii) For every $x \notin L$, it holds that $\Pr[M(x) = 0] \geq 1 - 2^{-p(|x|)}$.

Hint: Similar to part (A) but use the stronger Chernoff bound (refer to [slides](#) or these [notes](#) for Chernoff).

Problem 6 (On Negligence). Recall the definition of negligible functions from [Definition 6, Lecture 3] for answering the questions below.

- a) Which of the following functions are negligible in terms of the security parameter n ? Formally prove or refute in each case.

- i) $\mu_1(n) := 1/n^{2^{100}}$
- ii) $\mu_2(n) := 1/n^{\log n}$
- iii) $\mu_3(n) := 1/(\log 3)^{\sqrt{n^{3/2}}}$
- iv) $\mu_4(n) := \begin{cases} 1/n^{3000}, & \text{if } n \text{ is a prime} \\ 1/2^n, & \text{otherwise} \end{cases}$

- b) If ν_1 and ν_2 are negligible functions, are the following functions always negligible? If yes, give a proof (by reduction), else give a counter-example:

- i) $f_+(n) := \nu_1(n) + \nu_2(n)$
- ii) $f_\times(n) := \nu_1(n) \times \nu_2(n)$
- iii) $f_\div(n) := \nu_1(n) \div \nu_2(n)$

Problem 7 (PRGs). You can use either of the two (equivalent) [Definitions 1 or 2, Lecture 4] for a PRG. Let $G : \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}$ be a pseudorandom generator (PRG). In each case below, answer whether G' is a PRG or not. If yes, give a proof; if not, show a counterexample.

- a) $G'(s) := G(s_1 \cdots s_{\lfloor n/2 \rfloor})$, where $s = s_1 \cdots s_n$. Assume for this part that $\ell(n) > 2n$.
- b) $G'(s) := G(0^{|s|} || s)$, where $||$ means concatenation.
- c) $G'(s || b) := G(s) || b$, where $b \in \{0, 1\}$.

$$d) G'(s) := \begin{cases} 0^{\ell(n)}, & s = 0^{|s|} \\ G(s), & \text{otherwise} \end{cases}$$

Problem 8 (Game-based vs Two-worlds Definition).

- a) There were two ways in which I stated the definition of pseudorandomness for PRGs on [Slide 5, Lecture 4]. These are restated below for your reference. For both definitions: let ℓ be a polynomial and let G be a deterministic polynomial-time algorithm such that for any n , and any $k \in \{0, 1\}^n$, $G(k) \in \{0, 1\}^{\ell(n)}$, where $\ell(n) > n$ (expanding).

- **Definition 1 (Two-worlds Definition).** G is pseudorandom according to the “two-worlds” definition if for every PPT adversary Eve , there exists a negligible function negl such that

$$\left| \Pr_{k \in_R \{0,1\}^n} [\text{Eve}(G(k)) = 1] - \Pr_{r \in_R \{0,1\}^{\ell(n)}} [\text{Eve}(r) = 1] \right| \leq \text{negl}(n)$$

- **Definition 2 (Game-based definition).** G is pseudorandom according to the “game-based” definition if for every PPT adversary Eve , there exists a negligible function negl such that

$$\Pr[\text{PR}_{\text{Eve}, G}(n) = 1] \leq 1/2 + \text{negl}(n),$$

where $\text{PR}_{\text{Eve}, G}(n)$ outputs 1 if and only if Eve wins in the following game: The challenger picks a random bit $b \in_R \{0, 1\}$ and sends $y_0 = G(k)$ for $k \in_R \{0, 1\}^n$, if $b = 0$ and $y_1 \in_R \{0, 1\}^{\ell(n)}$, if $b = 1$. Eve then outputs b' and wins the game if $b' = b$.

Prove that Definitions 1 and 2 above are equivalent.

- b) Write down a similar two-worlds definition for computational security, which will be equivalent to the computational indistinguishability one [Definition 7, Lecture 3] via a similar argument as you gave in part a).

Problem 9 (Unpredictability vs Pseudorandomness). Recall [Definition 1, Lecture 4] (Next-bit Unpredictability) and [Definition 2, Lecture 4] (Pseudorandomness). Now let us define first-bit unpredictability exactly like Definition 1 for (next-bit) unpredictability for $G : \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}$: the predictor Eve^{pred} can ask for bits $y_2, \dots, y_i$ for any $i \in \{2, \dots, \ell(n)\}$ of its choice and has to predict the first bit y_1 .

- a) Show that if a PRG G is pseudorandom (by Def 2), then it is also first-bit unpredictable.
- b) Does the converse hold? That is, does first-bit unpredictability imply pseudorandomness? Either prove it or give a counter-example.
- c) Does first-bit unpredictability imply next-bit unpredictability? Either prove it or give a counter-example.

Problem 10 (Transitivity of indistinguishability). Recall the definition of computational indistinguishability from [Definition 7, Lecture 3] for encryption security. We can generally define computationally indistinguishability (CI) of two distributions X and Y as follows: for every PPT adversary Eve , there exists a negligible function negl such that

$$\left| \Pr_{x \leftarrow X} [\text{Eve}(x) = 1] - \Pr_{y \leftarrow Y} [\text{Eve}(y) = 1] \right| \leq \text{negl}(n)$$

Show formally that computational indistinguishability is a transitive property, i.e., if X_1 is CI from X_2 , and X_2 is CI from X_3 , then X_1 is CI from X_3 .