CS 409M : Introduction to Cryptography Fall 2024

Assignment 2
Enter the Security of Cryptosystems

Instructor: Sruthi Sekar *TAs:* Giriraj Singh, Gyara Pragathi, Nilabha Saha

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: Truly Secure One-Time Pad?

When using the one-time pad with the key $k = 0^\ell$, we have $\mathtt{Enc}_k(m) = k \oplus m = m$ and the message is sent in the clear! It has therefore been suggested to modify the one-time pad by only encrypting with $k \neq 0^\ell$ (i.e., to have $\mathtt{Gen}$ choose k uniformly from the set of *nonzero* keys of length ℓ). Is this modified scheme still perfectly secure? Explain.

Problem 3: Bounds for Perfect Indistinguishability

Prove that a scheme satisfying Definition 2.5 (from the book[1]):

Definition 2.5

Encryption scheme $\Pi = (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ with message space $\mathcal{M}$ is perfectly indistinguishable if for every $\mathcal{A}$ it holds that

$$\mathbb{P}[\mathtt{PrivK}^{\mathtt{eav}}_{\mathcal{A},\Pi} = 1] = \frac{1}{2}.$$

must have $|\mathcal{K}| \geq |\mathcal{M}|$ without using Lemma 2.6 (from the book):

Lemma 2.6

Encryption scheme Π is perfect secret if and only if it is perfectly indistinguishable.

Specifically, let Π be an arbitrary encryption scheme with $|\mathcal{K}| < |\mathcal{M}|$. Show an $\mathcal{A}$ for which $\mathbb{P}[\mathtt{Priv}^{\mathtt{eav}}_{\mathcal{A},\Pi} = 1] > \frac{1}{2}$.
Hint: It may be easier to let $\mathcal{A}$ be randomised.

Problem 4: Correctness with Errors

Assume we require only that an encryption scheme $(\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ with message space $\mathcal{M}$ satisfy the following: For all $m \in \mathcal{M}$, we have $\mathbb{P}[\mathtt{Dec}_K(\mathtt{Enc}_K(m)) = m] \geq 2^{-t}$. (This probability is taken over 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.

[1] Introduction to Modern Cryptography, Second Edition - Jonathan Katz, Yehuda Lindell

Problem 5: ϵ-Perfect Secrecy

Let $\epsilon \geq 0$ be a constant. Say an encryption scheme is *ϵ-perfectly secret* if for every adversary $\mathcal{A}$ it holds that

$$\mathbb{P}[\mathtt{Priv}^{\mathtt{eav}}_{\mathcal{A},\Pi} = 1] \leq \frac{1}{2} + \epsilon.$$

Show that for ϵ-perfectly secure encryption (with $\epsilon > 0$), $|\mathcal{K}| \geq (1 - \epsilon) \cdot |\mathcal{M}|$.

Problem 6: 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 the compute ciphertexts $c_1 \leftarrow \mathtt{Enc}_k(m_1)$ and $c_2 \leftarrow \mathtt{Enc}_k(m_2)$; this induces a distribution over pairs of ciphertexts and we let C_1, C_2 be the corresponding random variables.

a) Say encryption scheme $(\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ 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 $(\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ 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 to be efficient, although an efficient solution is possible.

Problem 7: BPP

(A) Recall Definition 5 from Lecture 4 for the complexity class BPP. Prove that $L \in \mathsf{BPP}$ (according to Definition 5), if there exists a polynomial $p(.)$ and a randomized Turing machine M such that

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

(B) Prove that for every $L \in \mathsf{BPP}$ (according to Definition 5, Lecture 4) and every $p(.)$, there exists a randomized Turing machine M such that

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

Problem 8: On Negligence

Which of the following functions are negligible in terms of the security parameter λ?

a) $2^{-\lambda}$

b) $1/\lambda^{2^{100}}$

c) $\lambda^{-\log \lambda}$

d) $(\log 3)^{-\sqrt{\lambda^{3/2}}}$

e) $5^{-3\lambda} + 45\lambda^{-\log \lambda}$

f) $(\lambda^{2^{160}} + 10^{100}\lambda^{40} + 70\lambda + 8) \cdot 2^{-\sqrt{\lambda}}$

Problem 9: `EAV-Security` Requires Equal-Length Outputs

Prove that Definition 3.8 (from the book):

Definition 3.8

A private key encryption scheme $\Pi = (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ has indistinguishable encryptions in the presence of an eavesdropper, or is `EAV-secure`, if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there is a negligible function `negl` such that, for all n,

$$\mathbb{P}[\mathtt{PrivK}^{\mathtt{eav}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathtt{negl}(n),$$

where the probability is taken over the randomness used by $\mathcal{A}$ and the randomness used in the experiment (for choosing the key and the bit b, as well as any randomness used by `Enc`).

cannot be satisfied if Π can encrypt arbitrary-length messages and the adversary is not restricted to output equal-length messages in experiment $\mathtt{PrivK}^{\mathtt{eav}}_{\mathcal{A},\Pi}$.
Hint: Let $q(n)$ be a polynomial upper-bound on the length of the ciphertext when Π is used to encrypt a single bit. Then consider an adversary who outputs $m_0 \in \{0,1\}$ and a uniform $m_1 \in \{0,1\}^{q(n)+2}$.