Homework 3

Due: October 4, 2024

CS 1510: Intro. to Cryptography and Computer Security

1 CPA Security from PRFs and PRGs

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF and $G : \{0,1\}^n \to \{0,1\}^{n+1}$ be a PRG with expansion factor $\ell(n) = n + 1$. Consider the following encryption schemes based on F and G, where in each case, the secret key is a uniform $k \in \{0,1\}^n$.

For each scheme, state 1) whether the scheme is semantically secure and 2) whether it is CPA-secure. Explain your answer **for each security definition** - if you think the scheme is secure under some definition, prove it; otherwise, give an attack.

a. To encrypt a message $m \in \{0,1\}^{n+1}$, choose a uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, G(r) \oplus m \rangle$.

b. To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$.

c. To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1 || m_2$ with $|m_1| = |m_2|$, then choose uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle$.

2 MAC from PRF

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF. Consider the following MAC constructions for fixed-length messages. In each case, Gen outputs a uniform random $k \in \{0,1\}^n$. We use $\langle i \rangle$ to denote an $\frac{n}{2}$-bit binary representation of the integer i. For each construction, either prove that it is necessarily a secure MAC, or provide a counterexample with an attack.

a. To authenticate a message $m = m_1, \ldots, m_\ell$, where $m_i \in \{0,1\}^n$, compute and output

$$t := F_k(m_1) \oplus \ldots \oplus F_k(m_\ell).$$

b. To authenticate a message $m = m_1, \ldots, m_\ell$, where $m_i \in \{0,1\}^{n/2}$, compute and output

$$t := F_k(\langle 1 \rangle || m_1) \oplus \ldots \oplus F_k(\langle \ell \rangle || m_\ell).$$

c. To authenticate a message $m = m_1, \ldots, m_\ell$, where $m_i \in \{0,1\}^{n/2}$, choose a uniform random $r \in \{0,1\}^n$, compute

$$t := F_k(r) \oplus F_k(\langle 1 \rangle || m_1) \oplus \ldots \oplus F_k(\langle \ell \rangle || m_\ell),$$

and let the output tag be $\langle r, t \rangle$.

3 Insecure Variable-Length CBC-MACs

In this problem, we will explore some nuanced difficulties with using CBC-MAC to authenticate messages of different lengths.

a. Consider the case in which the sender and receiver do not agree on the message length in advance. In this case, we have $\mathsf{Verify}_k(m, t) = 1$ if and only if $t = \mathsf{Mac}_k(m)$, regardless of the length of m. Say the sender is careful to only authenticate messages of length $2n$. Show that an adversary can forge a valid tag on a message of length $4n$.

b. Say the receiver only accepts 3-block messages. In this case, we have $\mathsf{Verify}_k(m, t) = 1$ if and only if $t = \mathsf{Mac}_k(m)$ *and* m has length $3n$. Say the sender authenticates messages of any length that is a multiple of n. Show that an adversary can forge a valid tag on a new message (of length $3n$).

4 Secure Arbitrary-Length CBC-MAC

Consider the following modification of the basic CBC-MAC construction. First, $\mathsf{Mac}_k(m)$ computes $k_\ell = F_k(\ell)$, where F is a PRF and ℓ is the length of m. Then, compute the tag using basic CBC-MAC with key k_ℓ. Verify is canonical verification.

Prove that this modification gives a secure MAC for arbitrary-length messages. For simplicity, assume all messages have length a multiple of the block length. You may assume fixed-length CBC-MAC is secure.

5 Summary Question

Summarize the most important insights from this week's material, including from the lectures, notes, textbooks, homework problems, and other resources you find helpful, into a one-page resource. We expect that these summary pages will help you with the take-home midterm and final. Please note this question is graded based on completion—we will not be checking it for correctness.