# CS 6222, Homework 4

Instructor: Wei-Kai Lin

Total points: 30. Points are noted after each problem.

**Problem 1** (2pt each). Let $f$ be a pseudorandom function. Show that each of the following MACs is insecure. (In each case $\mathsf{Gen}$ outputs a uniform $k \leftarrow \{0,1\}^n$; we let $\langle i \rangle$ denote an $n/2$-bit encoding of the integer $i$.)

(a) To authenticate a message $m = m_1, ..., m_\ell$, where $m_i \in \{0,1\}^n$, compute $t := f_k(m_1) \oplus \cdots \oplus f_k(m_\ell)$.

(b) To authenticate a message $m = m_1, ..., m_\ell$, where $m_i \in \{0,1\}^{n/2}$, compute $t := f_k(\langle 1 \rangle \| m_1) \oplus \cdots \oplus f_k(\langle \ell \rangle \| m_\ell)$.

(c) To authenticate a message $m = m_1, ..., m_\ell$, where $m_i \in \{0,1\}^{n/2}$, choose uniform $r \leftarrow \{0,1\}^n$, compute $t := f_k(r) \oplus f_k(\langle 1 \rangle \| m_1) \oplus \cdots \oplus f_k(\langle \ell \rangle \| m_\ell)$, and let the tag be $(r, t)$.

[KL, Exercise 4.6]

**Problem 2** (4pt). Can the following problem be solved in polynomial time? Given a prime $p$, an integer $e \in Z^*_{p-1}$, and $y := g^e \mod p$ where $g$ is a uniform value in $Z^*_p$, find $g$; that is, compute $y^{1/e} \mod p$. If your answer is "yes," give a polynomial-time algorithm. If your answer is "no," show a reduction to one of the assumptions introduced in [KL, Chapter 9]. [KL, Exercise 9.21]

**Problem 3** (3pt each). Consider the following construction (a generalization of the collision-resistant hash function discussed in class and in [KL, Construction 9.78]).

**Construction.** Define a hash function $(\mathsf{Gen}, H)$ parameterized by an integer $t \in \mathbb{N}$ as follows:

- $\mathsf{Gen}$: on input $1^n$, run the cyclic group sampling to obtain $(G, q, g, h_2, ..., h_t)$ where $q$ is $n$-bit prime, the order of $G$ is $q$, $g$ is a generator of $G$, and $h_i$ is sampled uniformly at random from $G$ for all $i = 2, ..., t$. Output $s := (G, q, g, h_2, ..., h_t)$ as the key.
- $H$: given a key $s = (G, q, g, h_2, ..., h_t)$ and input $(x_1, ..., x_t)$ with $x_i \in Z_q$, output

$$H_s(x_1, ..., x_t) := g^{x_1} \prod_{i=2}^{t} h_i^{x_i}.$$

(a) Prove that if the discrete-logarithm problem is hard relative to $G$ and $q$ is prime, then for any $t$ that is a polynomial of $n$, this construction is a collision-resistant hash function.

(b) Notice that the output of $H$ is an element of $G$, but the number of bits needed to represent an element can be longer than $n$ (even $q$ is $n$-bit). Discuss how this construction can be used to obtain compression regardless of the number of bits needed to represent elements of $G$ (as long as it is polynomial in $n$).

[KL, Exercise 9.28]

**Problem 4** (4pt). Read Section 6.2, "The Merkle-Damgård Transform," of [KL] and answer the following.

Generalize the Merkle–Damgård transform to the case where $(\mathsf{Gen}, h)$ takes inputs of length $n+1$ and generates outputs of length $n$. (The hash function you construct should accept inputs of any length $L < 2^n$.) Prove that your transform yields a collision-resistant hash function for arbitrary-length inputs if $(\mathsf{Gen}, h)$ is collision resistant. [KL, Exercise 6.5]

**Problem 5** (4pt)**.** Given a computable function $\mathsf{Com}$, some polynomial $l(\cdot)$, the definition of perfect binding and hiding are

1. Perfect binding: For all $n \in \mathbb{N}$ and all $v_0, v_1 \in \{0,1\}^n$ such that $v_0 \neq v_1$, $r_0, r_1 \in \{0,1\}^{l(n)}$, it holds that $\mathsf{Com}(v_0, r_0) \neq \mathsf{Com}(v_1, r_1)$.
2. Perfect hiding: For all unbounded distinguisher $D$, for all $n \in \mathbb{N}$, $v_0, v_1 \in \{0,1\}^n$,

$$\Pr[r \leftarrow \{0,1\}^{l(n)} : D(\mathsf{Com}(v_0, r)) = 1] = \Pr[r \leftarrow \{0,1\}^{l(n)} : D(\mathsf{Com}(v_1, r)) = 1]$$

Prove that there do not exist a commitment scheme $\mathsf{Com}$ that satisfies both perfect binding and perfect hiding.

**Problem 6** (3pt each)**.** The zero-knowledge proof (ZKP) of Graph 3-Coloring and thus ZKP for any language in NP can be abstracted as follows. Let $L$ be a language in class NP, and let $x \in L$ and $w$ is a witness of $x$. The ZKP protocol $(P, V)$ proceed as below.

1. $P(x, w)$ computes $(\mathsf{state}, m_1)$ and then sends message $m_1$ to $V$.
2. $V(x)$ samples message $m_2$ uniformly at random and then sends $m_2$ to $P$ *without the need to look at* $m_1$.
3. $P(x, w)$ uses $(\mathsf{state}, m_2)$ and then computes and sends $m_3$ to $V$.

   (Afterward, $V$ checks the consistency of $(x, m_1, m_2, m_3)$ and then Accepts or Rejects.)

This is known as "sigma protocol," and it is useful to observe that $m_2$ is uniform and independent of $m_1$. The communication cost of the protocol is the total message length, denoted as $C(P, V) := |m_1| + |m_2| + |m_3|$.

Using the abstraction, consider the composition of two ZKP of two NP languages $L_a, L_b$. Suppose that $(P_a, V_a)$ is a ZKP of $L_a$ and $(P_b, V_b)$ is a ZKP of $L_b$.

(a) Construct a ZKP protocol such that a prover can efficiently convince a verifier that

"$x_a \in L_a$ AND $x_b \in L_b$"

when the prover is given the two witnesses $w_a$ of $x_a$ and $w_b$ of $x_b$. Show that the communication cost is $C(P_a, V_a) + C(P_b, V_b)$. Prove the completeness, soundness, and zero-knowledge.

(b) Construct a ZKP protocol such that a prover can efficiently convince a verifier that

"$x_a \in L_a$ OR $x_b \in L_b$"

when the prover is given only either $w_a$ or $w_b$. Show that the communication cost is $C(P_a, V_a) + C(P_b, V_b)$. Prove the completeness, soundness, and zero-knowledge. Specifically by zero-knowledge, the verifier shall not learn which of $(x_a, x_b)$ is in the corresponding language. Hint: assume that both protocols $(P_a, V_a)$ and $(P_b, V_b)$ send their $m_2$'s of the same length, and then consider that the verifier sends only one $m_2$ so that the prover is allowed to respond arbitrarily on one of the two instances; since $m_2$ is uniform and independent in both protocols, the completeness and soundness are almost direct, but ZK is challenging.