Homework 2

Cryptography & Network Security
CS 406 : Fall 2018

Released: Fri Sep 28
Due: Fri Oct 12

Rabin OWF, CCA Secure PKE, Hash Functions [Total 100 pts]

1. **2-Universal Hash Function.** [20 pts]

   For a prime number q and positive integers m, n, and $R := \mathbb{Z}_q^n$. Below, all probabilities refer to the uniformly random choice of $\mathbf{L} \leftarrow \mathbb{Z}_q^{n \times m}$, and all addition and multiplication of numbers are modulo q.

   (a) Suppose $D = \mathbb{Z}_q^m \setminus \{0^m\}$. Prove that $\forall \mathbf{x} \in D, \mathbf{a} \in R$, $\Pr_{\mathbf{L}}[\mathbf{Lx} = \mathbf{a}] = 1/|R|$.

   Hint: Fix an i s.t. $\mathbf{x}_i \neq 0$. Consider sampling $\mathbf{L}$ by picking the i^{th} column last.

   (b) Now suppose $D = \{0,1\}^m \setminus \{0^m\}$ (i.e., non-zero vectors with only 0 and 1 entries). Show that $\forall \mathbf{x}, \mathbf{y} \in D$ s.t. $\mathbf{x} \neq \mathbf{y}$, $\mathbf{a}, \mathbf{b} \in R$, $\Pr_{\mathbf{L}}[\mathbf{Lx} = \mathbf{a}, \mathbf{Ly} = \mathbf{b}] = 1/|R|^2$.

   Hint: Argue that if $\mathbf{x} \neq \mathbf{y}$ and $\mathbf{x}, \mathbf{y} \in \{0,1\}^m$ there are at least two coordinates i, j restricted to which $\mathbf{x}, \mathbf{y}$ are linearly independent. Consider sampling $\mathbf{L}$ by picking these two columns last.

   This shows that the family of functions $\mathcal{H} = \{h_{\mathbf{L}} \mid \mathbf{L} \in \mathbb{Z}_q^{n \times m}\}$, where $h_{\mathbf{L}} : D \to R$ is defined as $h_{\mathbf{L}}(\mathbf{x}) = \mathbf{Lx}$ is a 2-universal hash function when $D = \{0,1\}^m \setminus \{0^m\}$. We can upgrade this to a 2-universal hash function family for $D = \{0,1\}^m$ (i.e., including the all-zero vector) by considering $h_{\mathbf{L},\mathbf{u}}(\mathbf{x}) = \mathbf{Lx} + \mathbf{u}$ over all $(\mathbf{L}, \mathbf{u}) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m$.

2. **Square Root modulo $N = PQ$ as hard as factorizing.** Consider sampling two random k-bit prime numbers $P \neq Q$, and setting $N = PQ$. Suppose we are given an algorithm A which, on being given N and a random $x \in \mathbb{QR}_N$, returns $y \in \mathbb{Z}_N$ such that with probability ϵ, $y^2 \equiv x \pmod N$. (The probability is over the choice of P, Q, x and the randomness used by the algorithm A.) Give an algorithm B which, on being given N as above, outputs the factors P, Q with probability at least $\epsilon/2$ (the probability being over the choice of P, Q and the randomness of B). [20 pts]

   Hint: Use the square-root finding algorithm A, to find "collisions" for the squaring function (use the Chinese Remainder theorem to argue that this works). Then turn the collisions into elements $a, b \in \mathbb{Z}_N$ such that $ab \equiv 0 \pmod N$. Then, show how to use such a pair to fatcorize N.

3. **Pitfalls in fiddling with CCA secure schemes.** To protect against packet corruptions while transmission, suppose one uses an "enhanced" PKE scheme $(\mathsf{KeyGen}, \mathsf{Enc}^*, \mathsf{Dec}^*)$, derived from a PKE scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ as follows. The ciphertext in the enhanced scheme consists of three ciphertexts independently generated as encryptions of the plaintext under the original scheme. i.e., $\mathsf{Enc}^*(m) = (c_1, c_2, c_3)$, where $c_i \leftarrow \mathsf{Enc}(m)$. For decryption, the three ciphertexts are decrypted. If at least two of the ciphertexts decrypt to the same message, that message is output as the decryption. Otherwise an error message is produced.

(a) Show that $(\mathsf{KeyGen}, \mathsf{Enc}^*, \mathsf{Dec}^*)$ is IND-CPA secure, if $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is. [15 pts]

Hint: Consider a series of a hybrid experiments, with the first corresponding to using $\mathsf{Enc}^*(m_0)$ in the CCA security experiment, the last one to using $\mathsf{Enc}^*(m_1)$, and any two adjacent hybrids differing by an encryption of the form $\mathsf{Enc}(m_b)$.

(b) Show that $(\mathsf{KeyGen}, \mathsf{Enc}^*, \mathsf{Dec}^*)$ is *not* IND-CCA secure, even if $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is. [5 pts]

4. **Hash Functions.** In this problem we consider hash functions on a finite domain (from $\{0,1\}^{n(k)}$ to $\{0,1\}^{m(k)}$).

(a) **Preimage collision resistance $\not\Longrightarrow$ Second-preimage collision resistance.** Suppose $\mathcal{H}$ is preimage collision resistant. Modify $\mathcal{H}$ to $\mathcal{H}'$ (possibly with a different domain), so that the latter remains preimage collision resistant, but is not second-preimage collision resistant. (You must prove that $\mathcal{H}'$ has both these properties.) [8 pts]

(b) **Second-preimage collision resistance $\not\Longrightarrow$ Preimage collision resistance.** Given a CRHF $\mathcal{H}$ which compresses by two bits (say from n bits to $n-2$ bits), construct a CRHF $\mathcal{H}'$ that compresses by one bit (say from $n+1$ bits to n bits), such that the function $f(h', x) = (h', h'(x))$ (where $h' \in \mathcal{H}'$) is **not** a OWF. (In both $\mathcal{H}$ and $\mathcal{H}'$, collision-resistance holds when the hash function is drawn uniformly at random from the family.) [12 pts]

Hint: Can you define h' so that it includes (disjoint) copies of h and a copy of an easy to invert one-to-one function? Why would this retain second-preimage collision resistance? Why would this destroy preimage collision resistance?

(c) **(Sufficiently Shrinking) CRHF implies OWF.** Show that if $\mathcal{H}$ is a CRHF from n bits to $n/2$ bits, then the function $f(h, x) = (h, h(x))$ is a OWF. [Extra Credit]

Hint: You may use the following intermediate steps. Below we say that "x has a collision under f" if there exists an $x' \neq x$ such that $f(x) = f(x')$.

i. *Let $\mathcal{H}$ be a CRHF and suppose that for every $h \in \mathcal{H}$ and every x, x has a collision under h. Show that the function $f(h, x) = (h, h(x))$ is a OWF.*
ii. *Now, suppose that for each $h \in \mathcal{H}$, all but a negligible fraction of x's have a collision under h. Show that the function $f(h, x) = (h, h(x))$ is a OWF.*
iii. *Finally, apply the above to the case of $f : \{0,1\}^n \to \{0,1\}^{n/2}$.*

5. **UOWHF vs. CRHF** In this problem we consider hash functions which take arbitrarily long strings as inputs. [20 pts]

(a) Suppose $\mathcal{H}$ is a CRHF family. Then show that the hash function family $\mathcal{H}' = \{h^2 | h \in \mathcal{H}\}$ is also a CRHF, where h^2 is defined by $h^2(x) = h(h(x))$.

(b) Suppose $\mathcal{H}_0$ is a UOWHF family. Use $\mathcal{H}_0$ to construct $\mathcal{H}$, so that $\mathcal{H}$ is still a UOWHF, but the hash function family $\mathcal{H}' = \{h^2 | h \in \mathcal{H}\}$ is not a UOWHF, where h^2 is defined by $h^2(x) = h(h(x))$.