COS 433: Cryptography — Princeton University
Homework 8 — Due: April 25, 2017, 11:59pm

Homework 8

1 Problem 1 (20 points)

(a) Let F_0, F_1 be two supposed one-way functions. Say you know that one of F_0, F_1 is a secure one-way function, but the other is not. However, you do not know which one. Construct a new one-way function F that is secure as long as at least one of F_0, F_1 are secure, but not necessarily both. Prove the one-wayness of F relying on just the security of F_0 *or* F_1

(b) Let $(\mathsf{Gen}_0, F_0, F_0^{-1}), (\mathsf{Gen}_1, F_1^{-1}, F_1^{-1})$ be two supposed trapdoor permutations, and suppose the domain for both trapdoor permutations is the same set $\mathcal{X}$ (since they are permutations, the co-domain is also $\mathcal{X}$). Suppose you are guaranteed that both are in fact permutations, but one of the two may be insecure. You do not know which one. Construct a new trapdoor permutation $(\mathsf{Gen}, F, F^{-1})$ that is secure as long as at least one of $(\mathsf{Gen}_0, F_0, F_0^{-1}), (\mathsf{Gen}_1, F_1, F_1^{-1})$ is secure, but not necessarily both.

(c) Let $(\mathsf{Gen}_0, \mathsf{Enc}_0, \mathsf{Dec}_0), (\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ be two public key encryption schemes. Suppose you are guaranteed that both are correct, in that decrypting an encryption of m recovers m. However, only one of the schemes is CPA-secure, and you don't know which. Construct a new encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ that is CPA secure, provided at least one of the two schemes is CPA-secure.

(d) Let $(\mathsf{Gen}_0, \mathsf{Sign}_0, \mathsf{Ver}_0), (\mathsf{Gen}_1, \mathsf{Sign}_1, \mathsf{Ver}_1)$ be two digital signature schemes. Suppose you are guaranteed that both are correct, in that signatures will verify. However, only one of the schemes is CMA-secure, and you don't know which. Construct a new signature scheme $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ that is CMA-secure, provided at least one of the two schemes is CMA-secure.

The constructions you present above are called *combiners*. With some extra work, the construction from part (a) can be turned into a *universal* one-way function: a one-way function that is secure, provided that *some* one-way function exists (but you don't need to know the one-way function). The same goes for the encryption combiner. Unfortunately, these universal constructions are of little use in practice.

2 Problem 2 (15 points)

In class, we saw how to construct CCA-secure public key encryption from trapdoor permutations. To encrypt, you choose a random r, and let $c_0 = F(\mathsf{pk}, r)$, and $c_1 = \mathsf{Enc}_{SKE}(H(r), m)$. That is, you "encrypt" r using the trapdoor permutation, and then you hash r with H, and encrypt the message m using $H(r)$ as the key. We showed that in the random oracle model, assuming F represents a trapdoor permutation and Enc_{SKE} is a CCA-secure secret key encryption scheme, the resulting construction is secure.

Show that if F is instead an injective trapdoor function, the scheme may not be secure. To do this, devise a secure injective trapdoor function $(\mathsf{Gen}, F, F^{-1})$ such that, when you plug into the construction above, the resulting scheme is not CCA secure. Hint: while correctness determines how F^{-1} behaves on valid outputs of F (that is, points of the form $F(\mathsf{pk}, x)$ for some x), on invalid points, F^{-1} can behave arbitrarily.

3 Problem 3 (35 points)

(a) One way to block the attack from Problem 2 is to have the decrypter verify that c_0 is a valid output of the trapdoor function. Explain how the decrypter, who knows the secret key sk to invert, can verify whether or not c_0 is a valid output of the trapdoor function.

(b) Show how, if the decrypter performs this check, a CCA adversary for the scheme in Problem 2 may be able to do the following: given a supposed output y, check if y is a valid output of F. The adversary does this by performing a CCA query. What properties of Enc_{SKE} — the underlying secret key CCA-secure encryption scheme — do you need to guarantee that the adversary correctly determines the validity of y?

(c) Construct an injective trapdoor function $(\mathsf{Gen}, F, F^{-1})$ that is insecure if you can test for validity. That is, $(\mathsf{Gen}, F, F^{-1})$ should satisfy the following:

(1) Correctness: $\Pr[F^{-1}(\mathsf{sk}, F(\mathsf{pk}, x)) = x : (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}()] = 1$

(2) Security: $(\mathsf{Gen}, F, F^{-1})$ is a secure injective trapdoor function

(3) Suppose the adversary, in addition to receiving pk and $y^* = F(\mathsf{pk}, x^*)$ for a random x^*, has access to an oracle that tells her whether or not a given y is a valid output of F. Then the adversary can determine x^* by craftily choosing several query values $y_1, ...,$ and testing if they are valid outputs of F.

Hint: consider the following injective TDF F built from a TDP F'. $F(\mathsf{pk}, x) = (F'(\mathsf{pk}, x), x_1)$. That is, F is just F', except that it additionally outputs the first bit of x. It is possible to prove that F is a secure injective TDF if F' is a TDP. Moreover, an output (y, b) is valid if and only if b is equal to the first bit of the pre-image of y.

Show how to build on this idea to construct a TDF F satisfying the properties needed above.

4 Problem 4 (30 points)

Consider the following modification of the scheme from Problem 2. Key generation is still just the key generation for the TDP.

- $\mathsf{Enc}(\mathsf{pk}, m)$: choose a random r, and let $c_0 = F(\mathsf{pk}, r)$. let $c_1 = \mathsf{Enc}_{SKE}(H(r),\ (m, r)\ )$. That is, use the hash of r to encrypt the pair (m, r). Output $c = (c_0, c_1)$.
- $\mathsf{Dec}(\mathsf{sk}, (c_0, c_1))$: First, use the procedure from problem 3a to determine if c_0 is a valid output of F. If not, abort and output $\perp$. Then, let $r = F(\mathsf{sk}, c_0)$. Let $(m, r') = \mathsf{Dec}_{SKE}(H(r), c_1)$. Finally, check that $r = r'$; if not, abort and output $\perp$. Finally, output m.

(a) Show that the scheme above is secure in the random oracle model by modifying the proof we saw in class. You should assume that $(\mathsf{Enc}_{SKE}, \mathsf{Dec}_{SKE})$ is a CCA-secure secret key encryption scheme, and that $(\mathsf{Gen}, F, F^{-1})$ is a secure injective trapdoor function (but not necessarily a permutation).

(b) **Bonus (10 Points)** Explain what goes wrong in the above proof if you used the original encryption scheme where $c_1 = \mathsf{Enc}_{SKE}(H(r), m)$ and you remove the check in decryption that $r = r'$. (We know the scheme might be insecure, so the proof *cannot* work in this case)

Thus, using the injective TDF from Diffie-Hellman we saw in class, we have a CCA-secure public key encryption scheme in the random oracle model.