Homework 2

Deadline: Oct 17, 2016

1. **PRFs and PRGs:**

   (a) (5 points) Let $\{f_s\}_s$ be a collection of PRFs. Is $\{g_s(x)\}_s$ also a collection of PRFs, where $g_s(x) = f_s(x) \| f_s(\bar{x})$? Prove or give a counterexample.

   (b) (5 points) Let G_1 and G_2 be PRGs. Is $G(s) = G_1(s) \| G_2(s)$ also a PRG? Prove or give a counterexample.

2. **Encryption and MACs:**

   (a) (15 points) Let $E_1 = (\mathbf{Gen}_1, \mathbf{Enc}_1, \mathbf{Dec}_1)$ and $E_2 = (\mathbf{Gen}_2, \mathbf{Enc}_2, \mathbf{Dec}_2)$ be two secret key encryption schemes such that one of them is **IND-CPA** secure, but you don't know which one. Using only E_1 and E_2, construct an **IND-CPA** secure encryption scheme.

   (b) (15 points) Let $M_1 = (\mathbf{Gen}_1, \mathbf{Sign}_1, \mathbf{Verify}_1)$ and $M_2 = (\mathbf{Gen}_1, \mathbf{Sign}_1, \mathbf{Verify}_1)$ be two MAC schemes such that one of them is **UF-CMA** secure, but you don't know which one. Using only M_1 and M_2, construct a **UF-CMA** secure MAC scheme.

3. **Restricted PRFs:** Consider the following notion of "Restricted PRFs", consisting of of three algorithms:

   - $\mathbf{Gen}(1^n)$: is a PPT algorithm that samples a PRF key $K \leftarrow \{0,1\}^n$.
   - $\mathbf{Restrict}(K, x)$: is a PPT algorithm that takes as input a PRF key K and a point x in the input space of the PRF and outputs a restricted key K_x.

- **Eval**(K_x, x') is a deterministic polynomial time algorithm that takes as input a restricted key K_x and an input x' and outputs an element y.

We require two properties:

- *Restricted Correctness*: on any input point $x' \neq x$, PRF evaluation using the restricted key K_x yields the same result as PRF evaluation using the (unrestricted) key K.
- *Restricted Pseudorandomness*: the output of the PRF on input x looks pseudorandom to any PPT adversary, even if the restricted key K_x is given to the adversary.

(a) (15 points) Devise a formal definition of restricted PRFs.

(b) (20 points) Show that the GGM construction that we have seen in class is a Restricted PRF. In particular, define the **Restrict** and **Eval** algorithms, and prove both properties (restricted correctness and restricted pseudorandomness).

4. **The Hybrid argument:** (10 points) For integers $a \leq b$, let $U_{a,b}$ denote the uniform distribution over the integers $x, a \leq x \leq b$. Now consider the following two distributions:

   (a) $U_{0,2^n-1}$

   (b) $U_{2^n,2^{n+1}-1}$

   Consider the following proof via hybrid argument to establish that $U_{0,2^n-1}$ and $U_{2^n,2^{n+1}-1}$ are indistinguishable: For $0 \leq i \leq 2^n$, let $H_i = U_{i,2^n-1+i}$. Clearly, $H_0 = U_{0,2^n-1}$ and $H_{2^n} = U_{2^n,2^{n+1}-1}$. Also, for every $i, H_i \approx H_{i+1}$ because they are statistically close. Therefore, $U_{0,2^n-1} \approx U_{2^n,2^{n+1}-1}$.

   Is the above a valid proof? Explain your answer.

5. **Sealed-bid auction:** (15 points) We want to design a sealed-bid auction scheme. Assume that the seller is honest and that the buyers make their bids in some pre-determined ordered fashion (e.g., the lexicographical ordering of their names). A natural security requirement from a sealed-bid auction scheme is that buyer i should not be able

to choose his bid based on the bid of buyers $j < i$, since otherwise the former can always outbid the latter. Now, consider the following proposal to perform a sealed-bid auction among n buyers:

The seller publishes a public key pk for the IND-CPA secure encryption scheme based on trapdoor permutations discussed in class. Each buyer sends the encryption $Enc(pk, x)$ of its bid x over a public channel (i.e., everyone can observe that encrypted bids), and then the seller decrypts all of these and awards the product to the highest bidder.

Does this proposal satisfy the security requirement of sealed bid auction? Explain your answer.

(Extra credit) **Pseudo-Random Generators and One-Way Functions**: (25 points) Let $f : \{0,1\}^{2n} \longrightarrow \{0,1\}^{2n}$ be a one-way function, and let $G : \{0,1\}^{n} \longrightarrow \{0,1\}^{2n}$ be a pseudorandom generator. Consider the function $h(x) = f(G(x))$.

Prove that h is a one-way function.

(**Hint:** In a proof by reduction, you will need to use an adversary for h to either break the one-wayness of f or the pseudorandomness of G.)