0368.4162 Foundations of Cryptography November 28, 2019

Problem Set 3

Due: December 12

Instructions:

- Type your solution and email it to "focf19hw@gmail.com", with subject "HW#, ID#, Name".
- You're encouraged to use latex. You can find on the webpage the assignment's tex file to help you.
- You can cooperate. However, you should write the solution by yourself, and list all collaborators for each question. Same goes for any external sources that you may use.
- Do not discuss solutions over the course's forum. You are more than welcome though to ask for clarifications regarding the questions themselves.

1. In class, we've seen the GGM PRF, where both the key s and the input x were of length n. We would like to extend this construction so that for keys $s \in \{0,1\}^n$, we can apply the function for inputs $x \in \{0,1\}^*$ of arbitrary length.

   (a) (10 pts) Consider applying the GGM function as is for inputs of arbitrary length. That is, for any $x \in \{0,1\}^*$, letting ℓ be the length of x and G a length doubling PRG, define

   $$F_s(x) := G_{x_\ell}(G_{x_{\ell-1}}(\cdots G_{x_2}(G_{x_1}(s))\cdots)) \ .$$

   Show that F is not a PRF. (Recall that $G_0(s)$ and $G_1(s)$ denote the first and second n-bit blocks of the output, respectively.)

   (b) (25 pts) Consider the following variant of GGM. Let $G : \{0,1\}^n \to \{0,1\}^{3n}$ be a length-tripling PRG, and denote by $G_0(s), G_1(s), G_2(s)$ the first, second, and third blocks of n output bits, respectively. For any $x \in \{0,1\}^*$, and letting ℓ be the length of x, define

   $$F_s(x) := G_2(G_{x_\ell}(G_{x_{\ell-1}}(\cdots G_{x_2}(G_{x_1}(s))\cdots)) \ .$$

   Show that F is a PRF.

2. Let $(Auth, Ver)$ be a MAC, and assume $Auth$ is deterministic (i.e., it does not toss any coins on its own) and that for secret key of size n it produces tags of size n.

   (a) (30 pts) Consider the function $G : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{3n}$ defined as:

   $$G(sk, r) = r, \langle Auth_{sk}(1), r\rangle, \langle Auth_{sk}(11), r\rangle, \ldots, \langle Auth_{sk}(1^{2n}), r\rangle \ ,$$

   where $\langle \cdot, \cdot \rangle$ denotes inner product modulo 2. Show that G is a PRG.[1]

   (b) (**Bonus**: 10 pts) Consider the function $G : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{3n+1}$ defined as:

   $$G(sk, r) = r, \langle Auth_{sk}(r), r\rangle, \langle Auth_{sk}(1), r\rangle, \langle Auth_{sk}(11), r\rangle, \ldots, \langle Auth_{sk}(1^{2n}), r\rangle \ .$$

   Prove that this function is also a PRG, or give a counter example.

[1] You're allowed to use (without proof) the fact that for any distribution X and jointly distributed bit B, if A distinguishes X, B from X, U_1 with advantage ε, there exists a predictor P that given X predicts B with probability $1/2 + \varepsilon/2$ (where P runs in time polynomially related to that of A).

3. Let H be a collision-resistant hash function that for a key $hk \in \{0,1\}^n$ maps $\{0,1\}^{2n}$ to $\{0,1\}^n$. We would like to use H to construct a new collision-resistant H^* for inputs of arbitrary length. We first focus on inputs whose length is a power of two, 2^ℓ for some ℓ. We consider the following construction (known as *Merkle's tree hash*).

   Given a key hk for H, and an input x of length 2^ℓ, consider the following labeling $\{L_v\}_v$ of the binary tree of depth ℓ whose nodes are represented by $\{v \in \{0,1\}^i, i \in \{0,\ldots,\ell\}\}$:

   - For every leaf $v \in \{0,1\}^\ell$, $L_v := x_v 0^{n-1}$ (the vth bit of x padded).
   - For every intermediate node, $L_v = H_{hk}(L_{v0} L_{v_1})$ (the hash of its sons).

   The hash $H^*_{hk}(x)$ is then set to be the root label L_ε.

   (a) (25 pts) Show that H^* is also collision resistant in the sense that it is hard to find to inputs $x \neq x'$ of *the same* length 2^ℓ, which collide under H^*_{hk}.

   (b) (10 pts) Briefly explain how to extend H^* to inputs of any size (not necessarily a power of two), and so that it is hard to find collisions $x \neq x'$ also for inputs that are not of the same length. No need to prove.