Foundation of Cryptography, Fall 2016 Beny Applebaum and Iftach Haitner

Problem set 3

December 7, 2016 Due: December 22

- Please submit the handout in class, or email me, in case you write in LaTeX.
- Write clearly and shortly using sub claims if needed. The emphasize in most questions is on the proofs (no much point is writing a “solution" w/o proving its correctness).
- For Latex users, a solution example can be found in the course web site.
- It is ok to work in (small) groups, but please write the id list of your partners in the solution file, and each student should write her solution by *herself* (joint effort is only allowed in the “thinking phase").
- The notation we use appears in the introduction part of the first lecture (*Notation* section).

1. In class we proved the security of the GGM construction under the assumptions that: (1) The distinguisher is non-adaptive and (2) The distinguisher distinguishes between the last two hybrids. Complete the security proof of the GGM construction for the general case without assuming (1) or (2). Guidance: As part of your answer you should describe an efficient algorithm $D'^{D}(i, y_1, \ldots, y_t)$ that gets as an input a hybrid index i, a vector of $2n$-bit strings and an oracle access to a t-time distinguisher D. The algorithm should generate answers to the queries asked by D with the following property. If the input $(y_1, \ldots, y_t) \leftarrow G^t(U_n^t)$ then the answers are distributed exactly as in the hybrid H_i and if $(y_1, \ldots, y_t) \leftarrow U_{2n}^t$ then the answers to the queries are distributed exactly as in the ensemble H_{i+1}.

2. Let $\mathcal{F} = \{\mathcal{F}_n = \{f \colon \{0,1\}^n \mapsto \{0,1\}^n\}\}_{n\in\mathbb{N}}$ be a PRF, and let $\mathcal{H} = \{\mathcal{H}_n = \{h \colon \{0,1\}^{2n} \mapsto \{0,1\}^n\}\}_{n\in\mathbb{N}}$ be an efficient pairwise-independent function family.[1] We would like to prove that the function family ensemble $\mathcal{F} \circ \mathcal{H} = \{\mathcal{F}_n \circ \mathcal{H}_n = \{f \circ h \colon f \in \mathcal{F}_n, h \in \mathcal{H}_n\}\}_{n\in\mathbb{N}}$ is a PRF mapping strings of length $2n$ to string of length n.[2]

   (a) Prove that function family ensemble $\{G_n = \Pi_n \circ \mathcal{H}_n\}_{n\in\mathbb{N}}$ is computationally indistinguishable (actually also statistically) indistinguishable from $\{\Pi_{2n,n}\}_{n\in\mathbb{N}}$.

   Do the above using the following proof methodology. Fix an q-query, deterministic oracle-aided algorithm A, and $n \in \mathbb{N}$.

      i. Describe a process S (i.e., an algorithm) that outputs a pair of values (x, y), and let (X, Y) be the random variable describing the output of S in a random execution. Show that X describes the view of A^g, for $g \leftarrow G_n$ (i.e., X lists the query/answer pairs in a an execution of A^g for a random $g \leftarrow G_n$). Similarly, show that Y describes the view of $\mathsf{A}^{\pi_{2n}}$, for $\pi_{2n} \leftarrow \Pi_{2n,n}$.

      ii. Bound the probability that $X \neq Y$. This is the hardest part of the question, and only doable if you have defined S above in a suitable way...
      Start with proving the claim assuming that A never makes a colliding query: $\mathsf{A}^{g=\pi\circ h}$ never makes two distinct queries x, x' with $h(x) = h(x')$.

      iii. Use question (4a) from Ex2 to bound the advantage that A has in distinguishing G_n from $\Pi_{2n,n}$.

      iv. Prove that for $q \in \mathrm{poly}$, no q-query algorithm (even a randomized one) distinguishes $\{G_n\}_{n\in\mathbb{N}}$ from $\{\Pi_{2n,n}\}_{n\in\mathbb{N}}$ with more than negligible advantage.

   (b) Use the above to prove that $\mathcal{F} \circ \mathcal{H}$ is a PRF.

3. Write a full proof for Claim 11 in Lecture 5.

4. Prove that the existence of collision-resistance hash function family (definition 12, lecture 5) implies the existence of one-way functions. Do the same for TCR (definition 33).

[1] Namely, the family $\mathcal{H}_n$, for each $n \in \mathbb{N}$, is pairwise independent.

[2] The symbol $\circ$ stands for function composition, e.g., $f \circ h(x) = f(h(x))$.