0368-4162-01: Foundation of Cryptography, Fall 2010
Instructors: Ran Canetti and Iftach Haitner

Problem Set 2

December 26, 2010 Due: Jan. 3, in class

1. (a) [**10 points**] Show that if there exist "not trivial" pseudorandom functions ensemble $\mathbb{F} = \{\mathbb{F}_n\}$ (i.e., the domain of $f \in \mathbb{F}_n$, is $\{0,1\}^{\ell(n)}$ for a polynomial-time computable $\ell(n) \in \omega(\log n)$), then there exist pseudorandom generators.

   Note that there are no assumptions on the output length of the functions. Also don't go through one-way functions, unless you like to fully prove that one-way functions imply pseudorandom generators...

   (b) [**10 points**] Show that if there exist pseudorandom permutations, then there exist pseudorandom permutations that are *not* strong pseudorandom permutations.

2. The GGM construction was presented in class as a construction of an efficient ensemble of function families $\mathbb{F} = \{\mathbb{F}_n\}$, where each $f \in \mathbb{F}_n$ is from $\{0,1\}^n$ to $\{0,1\}^n$.

   We wish to construct an efficient ensemble $\mathbb{F}' = \{\mathbb{F}'_n\}$, where each $f \in \mathbb{F}_n$ is from $\{0,1\}^*$ to $\{0,1\}^n$, and the ensemble should be computational indistinguishable form the ensemble of random functions with the same domain/range.

   (a) [**20 points**] The GGM construction naturally works for inputs of any length (i.e., on input x, $F_s(x)$ outputs $f_x(s)$, where f is as defined in class). Is the resulting ensemble pseudorandom? If not, suggest a construction that works.

   (b) [**10 points**] How can we extend the *range* of the functions in the families in the GGM construction, say double the length?

3. Recall that a family of functions $\mathcal{H} = \{h : \{0,1\}^n \to \{0,1\}^m\}$ is pairwise independent, if for any for any $x \neq x' \in \{0,1\}^n$ it holds that

   $$\Pr_{h \leftarrow \mathcal{H}}[h(x) = h(x')] = 2^{-m}$$

   (That is, the probability that two fixed points in the domain collide under h is exactly the same as if h were a truly random function from $\{0,1\}^n$ to $\{0,1\}^m$.)

   (a) [**10 points**] There are many combinatorial constructions of efficient ensembles of pairwise independent hash functions with short description, in the following we consider one such a family.

Let $\mathcal{A}_{n\times m}$ be the set of all $n \times m$ binary matrices. Show that the family $\mathcal{H} := \{h_{A,b} \colon A \in \mathcal{A}_{n\times m}, b \in \{0,1\}^m\}$, where $h_{A,b}(x) \equiv Ax + b \bmod 2$, is pairwise independent.

(b) [**20 points**] Let $\ell(n) \in \omega(\log n)$ be a polynomial-time computable function. Show how to modify the GGM construction of pseudorandom function families so that an evaluation of $f \in \mathbb{F}_n$ on $x \in \{0,1\}^n$, would involve only $\ell(n)$ applications of the underlying length-doubling pseudorandom. generator.

Hint: Use pairwise independent ensembles.

4. Recall that a MAC is a trippet of PPT $(\mathsf{Gen}, \mathsf{Mac}, \mathsf{Ver})$ such that

(a) $\mathsf{Gen}(1^n)$ outputs a key $k \in \{0,1\}^*$

(b) $\mathsf{Mac}(k,m)$ where $m \in \{0,1\}^*$ and k generated by Gen, outputs a tag t. We sometimes write $\mathsf{Mac}_k(m)$

(c) $\mathsf{Ver}(k,m,t)$ outputs 1 (YES) or 0 (NO). We sometimes write $\mathsf{Ver}_k(m,t)$

We require

Consistency: $\mathsf{Ver}_k(m,t) = 1$ for any $k \in \mathrm{Supp}(\mathsf{Gen}(1^n))$, $m \in \{0,1\}^*$ and $t = \mathsf{Mac}_k(m)$

Unforgability: No PPT wins the MAC game against $(\mathsf{Gen}, \mathsf{Mac}, \mathsf{Ver})$ with more than negligible probability.

where the MAC game is defined as

Definition 1 (MAC game)**.** *Let $K_n = \mathsf{Gen}(1^n)$. An oracle-aided algorithm A wins the MAC game against* $(\mathsf{Gen}, \mathsf{Mac}, \mathsf{Ver})$*, if the following holds:*

$$(m,t) \leftarrow A^{\mathsf{Mac}_{K_n}, \mathsf{Ver}_{K_n}}(1^n) \colon \mathsf{Ver}_{K_n}(m,t) = 1 \wedge \mathsf{Mac}_{K_n} \textit{ was not asked on } m$$

(a) [**10 points**] The *strong* MAC game is defined as:

Definition 2 (Strong MAC game)**.** *Let $K_n = \mathsf{Gen}(1^n)$. An oracle-aided algorithm A wins the MAC game against* $(\mathsf{Gen}, \mathsf{Mac}, \mathsf{Ver})$*, if the following holds:*

$$(m,t) \leftarrow A^{\mathsf{Mac}_{K_n}, \mathsf{Ver}_{K_n}}(1^n) \colon \mathsf{Ver}_{K_n}(m,t) = 1 \wedge \mathsf{Mac}_{K_n} \textit{ was not asked on } m \textit{ and replied with } t$$

That is, A wins the game even if it creates a different tag for a message on which it did queried Mac_{K_n}.

Let A be an algorithm that on security parameter n, makes at most $q(n)$ queries to Ver and wins the strong MAC game against $(\mathsf{Gen}, \mathsf{Mac}, \mathsf{Ver})$ with probability $\varepsilon(n)$.

Assuming that $q(n)$ is polynomial-time computable, construct an algorithm A', whose running time is essentially the same as of A, that makes *no* queries to Ver, and breaks the same MAC game with probability at least $\varepsilon(n)/(q(n)+1)$.

(b) [**10 points**] Let $\ell(n) \in \omega(\log n)$ be a polynomial-time computable function. Show how to construct a zero-time MAC (i.e., the adversary is not allowed to make any Mac-queries) whose key length (on security parameter n) is $\ell(n)$.

Restriction: use no assumptions (e.g., PRG exist).

5. [**Bonus: 20 points**] An efficient function family ensemble $\mathbb{F} = \{\mathbb{F}_n\}_{n \in \mathbb{N}}$, $\mathbb{F}_n = \left\{f \colon \{0,1\}^* \mapsto \{0,1\}^{l(n)}\right\}$, is called $\mathsf{weakly\ collision\ resistant}$, if the following holds for any PPT A and large enough n

$$\Pr_{f \leftarrow \mathbb{F}_n}[(x, x') \leftarrow A(1^n, f) \colon x \neq x' \wedge f(x) = f(x')] \leq 1/2$$

Show that if there exists such ensemble, then there exists efficient collision resistant function family ensembles in the standard (strong) sense we defined in class.

Hint: in the constructed family, the output will be longer than in the original family. How much larger will it have to be?