CS 601.442/642 – Modern Cryptography Instructor: Abhishek Jain

Midterm Exam

There are six questions below. **You are only required to answer five of them**. Please circle the numbers of the five questions you would like to be graded on.

1. For any one-way function $f : \{0,1\}^n \rightarrow \{0,1\}^{2n}$, define $g : \{0,1\}^n \rightarrow \{0,1\}^n$ s.t. $g(x) = f(x)[1:n]$, where $a[1:n]$ denotes the first n bits of a. Let $h : \{0,1\}^n \rightarrow \{0,1\}^n$ be a one-way function. **Prove** that you can construct a one-way function f' such that $g(x) = f'(x)[1:n]$ is **not** a one-way function.

   paces

2. Define a family of PRFs $\{F_k\}_{k \in \{0,1\}^{4n}}$ where $F_k : \{0,1\}^4 \rightarrow \{0,1\}^n$. We can write each key k as $k_0||k_1||k_2||k_3$, where each k_i is n bits long. Then, define F as:

$$F_k(x) = \bigoplus_{i:x_i=1} k_i$$

   For example, if $x = 1101$, then $F_k(x) = k_0 \oplus k_1 \oplus k_3$.

   Prove that F is **not** a secure PRF.

3. Let $\mathbb{G}$ be a cyclic group of prime order q with generator g. Give a proof sketch showing that for $x_1, x_2, x_3, ..., x_n, r_1, r_2, ..., r_{n-1} \xleftarrow{\$} \mathbb{Z}_q$ the following two distributions are indistinguishable.

$$D_1 = (g^{x_1}, g^{x_2}, g^{x_3}, ..., g^{x_n}, g^{x_1 x_2}, g^{x_2 x_3}, ..., g^{x_{n-1}, x_n})$$
$$D_2 = (g^{x_1}, g^{x_2}, g^{x_3}, ..., g^{x_n}, g^{r_1}, g^{r_2}, ..., g^{r_{n-1}})$$

   Your proof sketch should contain a description of the relevant hybrids, but the indistinguishability of the hybrids can be sketched.

4. Let $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be a *Multi-message IND-CPA Secure* encryption scheme. Define a new encryption scheme $\mathcal{E}'$ as follows:

   - $\mathsf{KeyGen}'(1^n)$:
     - $k \leftarrow \mathsf{KeyGen}(1^n)$
     - $t \xleftarrow{\$} \{0,1\}^n$
     - Output (k, t)
   - $\mathsf{Enc}'((k,t), m)$:
     - If $m == t$, set $c := 0||\mathsf{Enc}(k, m)$
     - Else, set $c := 1||\mathsf{Enc}(k, m)$
     - Output (c, t)
   - $\mathsf{Dec}'((k,t),(c,t))$:
     - Output $\mathsf{Dec}(k, c[1:])$

   Observe that both the key AND the ciphertexts contain the value t.

   Explain why $\mathcal{E}'$ is **not** a *Multi-message IND-CPA Secure* encryption scheme.

   Note that when we first introduced IND-CPA security in class we referred to it as *Multi-message Secure Encryption*.

5. We saw in class a way to take a PRG G with one-bit strech and use it to construct a PRG G' with multi-bit stretch. The construction was as follows:

   $G'(s)$:

   - $x_0 := s$
   - $x_1||b_1 \leftarrow G(x_0)$
   - $x_2||b_2 \leftarrow G(x_1)$
   - ...
   - $x_{\ell(n)}||b_{\ell(n)} \leftarrow G(x_{\ell(n)-1})$
   - Output $b_1||b_2||...||b_{\ell(n)}$

   (a) Consider a new construction for a multi-bit stretch PRG G_1:

   $G_1(s)$:

   - $x_0 := s$
   - $x_1||b_1 \leftarrow G(x_0)$
   - $x_2||b_2 \leftarrow G(x_1)$
   - ...
   - $x_{\ell(n)}||b_{\ell(n)} \leftarrow G(x_{\ell(n)-1})$
   - Output $b_1||b_2||...||b_{\ell(n)}||x_{\ell(n)}$

   Explain why G_1 **is** a secure PRG.

   (b) Consider a new construction for a multi-bit stretch PRG G_2:

   $G_2(s)$:

   - $x_0 := s$
   - $x_1||b_1 \leftarrow G(x_0)$
   - $x_2||b_2 \leftarrow G(x_1)$
   - ...
   - $x_{\ell(n)}||b_{\ell(n)} \leftarrow G(x_{\ell(n)-1})$
   - Output $b_1||b_2||...||b_{\ell(n)}||x_1$

   Explain why G_2 is **not** a secure PRG.

6. Recall that in our security definitions, we model adversaries as *non-uniform* PPT machines. A way to think about non-uniformity is that it allows the adversary to receive an additional polynomial-size input, namely, an *advice*, that need not be efficiently computed.

   For any PRG $G : \{0,1\}^n \rightarrow \{0,1\}^{n+\ell}$ there will be many strings in $\{0,1\}^{n+\ell}$ that are not possible to get as an output of G. Let S be the set of impossible G-outputs. We could use S as the *advice* for a PRG adversary $\mathcal{A}$ that on receiving the challenge x from the challenger simply checks if $x \in S$, and if so guesses that x was sampled from the uniform distribution over $\{0,1\}^{n+\ell}$ rather than generated by G.

   (a) What is the advantage of $\mathcal{A}$?

   (b) Why does the existence of $\mathcal{A}$ not break the security of every PRG?