EE 720: An Introduction to Number Theory and Cryptography (Spring 2018)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Quiz 1 : 20 points February 16, 2018

1. (5 points) Consider a modification to the one-time pad where the message space $\mathcal{M} = \{0,1\}^n$ and the key space $\mathcal{K}$ consists of all n-bit strings with an even number of ones. We know that this scheme is not perfectly secure as the key space is smaller than the message space. Define a probabilistic polynomial time adversary $\mathcal{A}$ in the experiment $\mathtt{PrivK}^{\mathtt{eav}}_{\mathcal{A},\Pi}$ who succeeds with probability 1 **for any** n (i.e. don't define an adversary only for a fixed value of n like 3).

2. (5 points) Let $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ be a pseudorandom generator with expansion factor $l(n) > n$. **Prove or disprove** that the following functions are pseudorandom generators where $s \in \{0,1\}^n$ and s_i is the ith bit of s.
   (a) $G_1(s) = G(s) \| 0$.
   (b) $G_2(s) = G(s_1, s_2, \ldots, s_{|s|-1}) \| s_{|s|}$.
   (c) $G_3(s) = G(s \| 0)$.

3. (10 points) If $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is a length-preserving keyed pseudorandom function, then prove that the below construction is a CPA-secure private-key encryption scheme for messages of length n.
   - `Gen`: On input 1^n, choose k uniformly from $\{0,1\}^n$.
   - `Enc`: Given $k \in \{0,1\}^n$ and message $m \in \{0,1\}^n$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext
   $$c := \langle r, F_k(r) \oplus m \rangle.$$
   - `Dec`: Given $k \in \{0,1\}^n$ and ciphertext $c = \langle r, s \rangle$, output the plaintext message
   $$m := F_k(r) \oplus s.$$