Cryptography, winter term 16/17: Assignment 3

Prof. Markus Bläser, Cornelius Brand, Marc Roth
http://www-cc.cs.uni-saarland.de/course/55/

Due November 23, 2016

Exercise 3.1 (Be nice to your tutors and TAs, 1 Bonus Point) Write the name and matriculation number of every author as well as number, time slot and the name of the tutor of your tutorial group on the first page of your solution. Furthermore write in english and staple *all* sheets of your solution.

Exercise 3.2 (Pseudorandom Generators, 2 + 6 Points) Let G be an *arbitrary* PRG with expansion factor $\ell(n) > 2n + 1$.

(a) Show that given a negligible function f, the function $f' : n \mapsto f(\lfloor \frac{n}{2} \rfloor)$ is also negligible and use this to prove that the following function is a PRG:

$$G' : s \mapsto G(s_1 \dots s_{\lfloor \frac{n}{2} \rfloor}) \text{ , where } s = s_1 \dots s_n$$

(b) Decide for each i whether G_i is always a PRG and prove your answer:

(i) $G_1(s) := G(0^{|s|}||s)$

(ii) $G_2(s) := G(s_1 \dots s_{|s|-1})||s_{|s|}$

(iii) $G_3(s) := G(s)||0$

(iv) $G_4(s) := G(s||0)$

(v) $G_5(s) := G(s)||G(s+1)$, where $+$ denotes the addition on binary numbers.

Hint: To prove that G_i is a PRG one *usually* gives a proof by reduction. To prove that G_i is not secure you can give a counter example, i.e. a PRG G and a ppt algorithm D such that D can distinguish $G_i(s)$ from a random sting with non-negligible probability (of course you have to prove this). You could try to construct a counter example by using a construction you already proved to result in a PRG.

Exercise 3.3 (Pseudorandom Functions, 4 Points) Consider the following keyed function F: For the security parameter n, the key is a matrix $A \in \mathrm{Mat}(n \times n, \mathbb{F}_2)$ and a vector $b \in \mathbb{F}_2^n$, where $\mathbb{F}_2$ denotes the field with 2 elements, i.e. $\mathbb{F}_2 = (\{0,1\}, \oplus, \cdot)$ and $\mathbb{F}_2^n$ denotes the corresponding vector space of dimension n. Now we define $F_{A,b} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ by

$$F_{A,b}(x) = Ax + b$$

Decide whether F is a pseudorandom function and prove your answer.

Exercise 3.4 (From PRFs to PRGs, 4 Points) Let F be a length-preserving PRF and let $[k]_2^n$ denote the n-bit binary expression of the number k. Show that the following function is a PRG with expansion factor $n \mapsto \ell \cdot n$:

$$G(s) := F_s([1]_2^{|s|})||F_s([2]_2^{|s|})|| \dots ||F_s([\ell]_2^{|s|})$$