Cryptography, winter term 16/17: Sample solution to assignment 3

Cornelius Brand, Marc Roth

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.

Solution 3.2 (Pseudorandom Generators, 2 + 6 Points)

(a) We first show that f' is negligible. Let therefore c be a natural number. We have to show that there is an N' such that for all $n > N'$ it holds that $f'(n) < n^{-c}$. As f is negligible and $p'(n) = 2^c \cdot (n+1)^c$ is a polynomial we conclude that there is an N such that for all $n > N$ it holds that $f(n) < p'(n)^{-1}$. Now let $N' := 2N + 1$. We have for all $n > N'$:

$$f'(n) = f\left(\left\lfloor \frac{n}{2} \right\rfloor\right) < p'\left(\left\lfloor \frac{n}{2} \right\rfloor\right)^{-1} = \left(2^c \cdot \left(\left\lfloor \frac{n}{2} \right\rfloor + 1\right)^c\right)^{-1} \leq \left(2^c \cdot \left(\frac{n}{2}\right)^c\right)^{-1} = n^{-c}$$

Next we proof that G' is a PRG. Let ℓ' be the expansion factor of G'. It holds that $\ell'(n) = \ell(\lfloor \frac{n}{2} \rfloor) > 2(\lfloor \frac{n}{2} \rfloor) + 1 \geq n$. Now let D an arbitrary ppt distinguisher. As G is a PRG it holds that

$$
\begin{aligned}
&\left|\Pr_{s\leftarrow\{0,1\}^n}[D(G'(s))=1]-\Pr_{r\leftarrow\{0,1\}^{\ell'(n)}}[D(r)=1]\right| \\
&=\left|\Pr_{s\leftarrow\{0,1\}^{\lfloor\frac{n}{2}\rfloor}}[D(G(s))=1]-\Pr_{r\leftarrow\{0,1\}^{\ell'(n)}}[D(r)=1]\right| \\
&=\left|\Pr_{s\leftarrow\{0,1\}^{\lfloor\frac{n}{2}\rfloor}}[D(G(s))=1]-\Pr_{r\leftarrow\{0,1\}^{\ell(\lfloor\frac{n}{2}\rfloor)}}[D(r)=1]\right| \\
&\leq \mathrm{negl}\left(\left\lfloor\frac{n}{2}\right\rfloor\right)
\end{aligned}
$$

where negl is a negligible function. As $\mathrm{negl}'(n) := \mathrm{negl}\left(\left\lfloor\frac{n}{2}\right\rfloor\right)$ is also negligible the proof is finished.

(b) Only G_2 is a PRG. In some of the refutation proofs we will use G' instead of G. To ensure that the expansion factor of G' is large enough we can just assume the expansion factor of G to be strictly larger than $4n+1$.

(i) G_1 is not necessarily a PRG because otherwise $G'(0^{|s|}||s) = G(0^{|s|})$ would also be a PRG which is clearly not the case: As D knows G and its expansion factor ℓ it can on input r just check whether $r = G(0^n)$ for n with $\ell(n) = |r|$. Then D wins with probability $1 - 2^{-|r|}$ which is not negligible.

(ii) G_2 is always a PRG. We give a proof by reduction: Assuming G_2 is not a PRG, there is a distinguisher D_2 for G_2 which wins with non-negligible probability. We construct a distinguisher D for G from D_2. On input r, D will just simulate D_2 on $r||b$ for a randomly choosen bit b. If r was a random string, then $r||b$ is also and if $r = G(s)$ for a random s then $r||b = G(s)||b = G_2(s||b)$. Formaly it holds that

$$
\begin{aligned}
&\left|\Pr_{s\leftarrow\{0,1\}^n}[D(G(s))=1]-\Pr_{r\leftarrow\{0,1\}^{\ell(n)}}[D(r)=1]\right| \\
&=\left|\Pr_{s||b\leftarrow\{0,1\}^{n+1}}[D_2(G(s)||b)=1]-\Pr_{r||b\leftarrow\{0,1\}^{\ell(n)+1}}[D_2(r||b)=1]\right| \\
&=\left|\Pr_{s||b\leftarrow\{0,1\}^{n+1}}[D_2(G_2(s||b))=1]-\Pr_{r\leftarrow\{0,1\}^{\ell(n)+1}}[D_2(r)=1]\right| \\
&=\left|\Pr_{s\leftarrow\{0,1\}^{n+1}}[D_2(G_2(s))=1]-\Pr_{r\leftarrow\{0,1\}^{\ell_2(n+1)}}[D_2(r)=1]\right| \\
&\geq (n+1)^{-c}
\end{aligned}
$$

(iii) G_3 is not a PRG as a distinguisher would just have to check whether the last bit is 0 and win with probability $\frac{1}{2}$ which is not negligible.

(iv) G_4 is not always a PRG because otherwise $G_2(s||0)$ would be a PRG (as G_2 is PRG). But $G_2(s||0) = G_3(s)$ which is not a PRG.

(v) G_5 is not always a PRG. Assuming it is $G_2(s)||G_2(s+1)$ would also be a PRG. But for every s whose last bit equals zero we have that $G_2(s)||G_2(s+1) = G(s_1 \dots s_{|s-1|})||0||G(s_1 \dots s_{|s-1|})||1$,that is, on input $r \in \{0,1\}^{2n}$ a distinguisher just has to check whether $r_1 \dots r_{n-1} = r_{n+1} \dots r_{2n-1}$ and therefore the winning probability is at least $\frac{1}{2}(1 - 2^{-(n-1)})$ which is not negligible.

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.

Solution 3.3 (Pseudorandom Functions, 4 Points) F is not a PRF. Consider the following distinguisher D:
First, D queries $F_{A,b}(0)$ which equals b, i.e., D can compute b with just one query. As b is known D can now compute Ax for every x. A boring, but absolutely right solution would be that D now computes A by posing queries for the unit vectors. Having A and b it is straight forward to continue.
Another solution (that does not need to query all unit vectors) would be to compute vectors v and w such that v, w and $v+w$ are pairwise distinct. As A is a linear mapping D has to check whether $Av + Aw = A(v+w)$. The winning probability for this is in fact $1 - 2^{-n}$ which is not negligible.

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 $n \mapsto \ell \cdot n$:

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

Solution 3.4 (From PRFs to PRGs, 4 Points) As F is length-preserving, the expansion factor follows immediately. We will prove that G is a PRG by reduction. Assume there is a ppt algorithm D that can distinguish between $G(s)$ and a random string r with non-negligible probability we construct an adversary D_F that can distinguish F from a random function as follows:
Given input 1^n and acces to an oracle $\mathcal{O}$, we compute $t = \mathcal{O}([1]_2^n) || \mathcal{O}([2]_2^n) || \dots || \mathcal{O}([\ell]_2^n)$ by posing ℓ queries for $\mathcal{O}$. Then we simulate D on t and output 1 if and only if D outputs 1. Now we have

$$\begin{aligned}
&\left|\Pr_{s \leftarrow \{0,1\}^n}[D_F^{F_s(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \mathrm{Func}_n}[D_F^{f(\cdot)}(1^n) = 1]\right| \\
&= \left|\Pr_{s \leftarrow \{0,1\}^n}[D(F_s([1]_2^{|s|}) || \dots || F_s([\ell]_2^{|s|})) = 1] - \Pr_{f \leftarrow \mathrm{Func}_n}[D(f([1]_2^n) || \dots || f([\ell]_2^n)) = 1]\right| \\
&= \left|\Pr_{s \leftarrow \{0,1\}^n}[D(G(s)) = 1] - \Pr_{r_1 \leftarrow \{0,1\}^n, \dots, r_\ell \leftarrow \{0,1\}^n}[D(r_1 || \dots || r_\ell) = 1]\right| \\
&= \left|\Pr_{s \leftarrow \{0,1\}^n}[D(G(s)) = 1] - \Pr_{r \leftarrow \{0,1\}^{\ell \cdot n}}[D(r) = 1]\right| \\
&\geq \frac{1}{n^c}
\end{aligned}$$

for a constant c as D has can distinguish with non-negligible probability by assumtion. Therefore D_F can also distinguish with non-negligible probability which concludes the reduction.