Solution

Cryptography – Homework 2

Discussed on Tuesday, 20th November, 2018.

Exercise 2.1 Negligible Functions

(a) Show that the following two definitions are equivalent:

i) $\varepsilon(n)$ is negligible if and only if $\forall a \in \mathbb{N} \exists N \in \mathbb{N} \forall n > N : \varepsilon(n) < n^{-a}$.

ii) $\varepsilon(n)$ is negligible if and only if $\forall$polynomials q $\exists N \in \mathbb{N} \forall n > N : \varepsilon(n) < \frac{1}{|q(n)|}$

(b) Let $\varepsilon_1 : \mathbb{N} \to \mathbb{R}^+, \varepsilon_2 : \mathbb{N} \to \mathbb{R}^+$ be negligible functions and let $p : \mathbb{N} \to \mathbb{R}^+$ be a polynomial in $\mathbb{R}$. Show that $f : \mathbb{N} \to \mathbb{R}^+$ with $f(n) = \varepsilon_1(n) + \varepsilon_2(n)$ and $g : \mathbb{N} \to \mathbb{R}^+$ with $g(n) = p(n) \cdot \varepsilon_1(n)$ are also negligible functions.

(c) Prove: If $\varepsilon_0, \varepsilon_1, \ldots$ is a family of negligible functions $\varepsilon_i \colon \mathbb{N} \to \mathbb{R}^+$ and $p \colon \mathbb{N} \to \mathbb{N}$ is a polynomial, then f with $f(n) := \sum_{i=0}^{n} \varepsilon_i(n)$ need not be negligible anymore.

Solution: A function $\varepsilon : \mathbb{N} \to \mathbb{R}^+$ is negligible iff for every polynomial $q(\cdot)$ there is an N s.t. $\forall n \geq N : \varepsilon(n) < 1/|q(n)|$. Let $q(\cdot)$ be an arbitrary polynomial.

(a) The second definition clearly implies the first one (n^a are just a special polynomials). Thus let us assume $\varepsilon(n)$ satisfies the first definition and show that it also satisfies the second one. To this end, fix some polynomial q. We can write q as $q(n) = a_K n^K + a_{K-1} n^{K-1} + \ldots a_1 n + a_0$. Since ε is negligible (according to the first def.) we know that $\varepsilon(n) < n^{-(K+1)}$ for n larger than some $N \in \mathbb{N}$. Since $n^{-(K+1)} < 1/|q(n)|$ for n larger than some other $N' \in \mathbb{N}$ we obtain that $\varepsilon(n) < 1/|q(n)|$ for $n > \max(N, N')$.

(b)
- Let $N_1, N_2 \in \mathbb{N}$ be such that for $i \in \{1, 2\}$, $\forall n \geq N_i : \varepsilon_i(n) < 1/|2q(n)|$. Now choose $N = \max(N_1, N_2)$ and let $n \geq N$. Then
$$f(n) = \varepsilon_1(n) + \varepsilon_2(n) < \frac{1}{|2q(n)|} + \frac{1}{|2q(n)|} = \frac{1}{|q(n)|}.$$
- Let N_1 be such that $\forall n \geq N_1 : \varepsilon_1(n) < 1/|p(n) \cdot q(n)|$. Now choose $N = N_1$ and let $n \geq N$. Then
$$g(n) = p(n) \cdot \varepsilon_1(n) < p(n) \cdot \frac{1}{|p(n) \cdot q(n)|} = \frac{1}{|q(n)|}$$
(note that $p(n) > 0$).

(c) Choose $\varepsilon_i(n) = \frac{2^i}{2^n}$ as family of negligible functions and let $p(n) = n$. Then
$$f(n) = \sum_{i=0}^{p(n)} \varepsilon_i(n) = \sum_{i=0}^{n} \frac{2^i}{2^n} = \frac{2^{n+1} - 1}{2^n} = 2 - \frac{1}{2^n}$$
Thus $\lim_{n\to\infty} f(n) = 2$ which implies that f is not negligible.

Exercise 2.2 Pseudorandom Generators

- Let $f \colon \{0,1\}^* \to \{0,1\}$ be any DPT-computable function.

  Show that $G_f(x) = x||f(x)$ is no PRG.
- Use a similar argument to show that also the follwing is not a PRG:

  Let $m \in \mathbb{N}$ and $a, c \in \mathbb{Z}_m$.
  - For simplicity, let $m = 2^n$ so that we may identify $\mathbb{Z}_m$ with $\{0,1\}^n$.

  For $x \in \{0,1\}^n$, let $f(x) = (a \cdot x + c) \bmod m$, and $G(x, 1^{n \cdot s}) = f(x)||f(f(x))|| \ldots ||f^s(x)$.

Solution: A possible $\mathcal{D}$ works as follows:

On input $y = y_1 \dots y_n y_{n+1} \in \{0,1\}^{n+1}$, output 1 iff $y_{n+1} = f(y_1 \dots y_n)$. Now:

(a) $\Pr_{b=1}\left[\mathsf{Win}_{n,G}^{\textsc{IndPRG}}(\mathcal{D})\right] = \Pr_{x \overset{u}{\in} \{0,1\}^n}[\mathcal{D}(G(x)) = 1] = 1$ by definition of G.

(b) $\Pr_{b=0}\left[\mathsf{Win}_{n,G}^{\textsc{IndPRG}}(\mathcal{D})\right] = \Pr_{y \overset{u}{\in} \{0,1\}^{n+1}}[\mathcal{D}(y) = 0] = 1/2$:

Given $y_1 \dots y_n$ the value $f(y_1 \dots y_n)$ is already fixed. As the last bit y_{n+1} is chosen uniformly and independent of the other bits, with prob. 1/2 we have $y_{n+1} = f(y_1 \dots y_n)$.

(c) Together we obtain: $\Pr\left[\mathsf{Win}_{n,G}^{\textsc{IndPRG}}(\mathcal{D})\right] = 1/2(1 + 1/2) = 3/4$ which is non-negligibly better than 1/2.

The second question works identically (it can even be seen as a special case of the first one).

Exercise 2.3 Pseudorandom Generators II

Let G be a PRG of stretch $l(n) = 2n$.

(a) Show that there exists an *exponential time* distinguisher $\mathcal{D}$ with:

$$\left|\Pr_{x \overset{u}{\in} \{0,1\}^n}[\mathcal{D}(1^n, G(x)) = 1] - \Pr_{y \overset{u}{\in} \{0,1\}^{2n}}[\mathcal{D}(1^n, y) = 1]\right| \geq 1 - 2^{-n}$$

(b) Determine the success probability of the following $\mathcal{D}$:

- Input: $y \in \{0,1\}^{l(n)}$ and 1^n.
- Generate $x' \overset{u}{\in} \{0,1\}^n$.
- Compute $y' = G(x')$.
- Return 1 if $y = y'$; else return 0.

Solution:

(a) The exponential time distinguisher works as follows: on input x check if $x \in G(\{0,1\}^n)$ (e.g. by enumerating all images of G). If so answer $r = 1$ else answer $r = 0$. If $b = 0$ then $\mathcal{D}$ will lose with probability at most $\frac{2^n}{2^{2n}} = 2^{-n}$ (i.e. the probability that a truly random string from $\{0,1\}^{l(n)}$ appears in the image of G).

If $b = 1$ it will win with probability 1.

(b) If $b = 1$, then $\mathcal{D}$ outputs 1 at least in those cases where it guesses to correct seed:

$$\Pr_{b=1}\left[\mathsf{Win}_{n,G}^{\textsc{IndPRG}}(\mathcal{D})\right] = \Pr_{x \overset{u}{\in} \{0,1\}^n}[\mathcal{D}(G(x)) = 1] \geq \Pr_{x \overset{u}{\in} \{0,1\}^n}[x' = x] = 2^{-n}$$

If $b = 0$, then – as the computation of $x' \overset{u}{\in} \{0,1\}^n; y' = G(x')$ is independent of $y \overset{u}{\in} \{0,1\}^{l(n)}$ – we can reorder the experiment so that first y' is generated, and only then y. As always the probability that $y \overset{u}{\in} \{0,1\}^{l(n)}$ "hits" any specific y' is $2^{-l(n)}$ because of the uniform distribution of y. More formally:

$$\Pr_{b=0}\left[\mathsf{Win}_{n,G}^{\textsc{IndPRG}}(\mathcal{D})\right] = 1 - \Pr_{y \overset{u}{\in} \{0,1\}^{l(n)}}[\mathcal{D}(y) = 1] = 1 - \sum_{y' \in G(\{0,1\}^n)} \Pr_{y \overset{u}{\in} \{0,1\}^{l(n)}, x' \overset{u}{\in} \{0,1\}^n}[y = y', G(x') = y']$$

$$\overset{y,x' \text{ indep.}}{=} 1 - \sum_{y' \in G(\{0,1\}^n)} \underbrace{\Pr_{y \overset{u}{\in} \{0,1\}^{l(n)}}[y = y']}_{=2^{-2n}} \Pr_{x' \overset{u}{\in} \{0,1\}^n}[G(x') = y'] = 1 - 2^{-2n} \underbrace{\sum_{y' \in G(\{0,1\}^n)} \Pr[G(x') = y']}_{=1} = 1 - 2^{-2n}$$

Together we obtain: $\Pr\left[\mathsf{Win}_{n,G}^{\textsc{IndPRG}}(\mathcal{D})\right] \geq \frac{1}{2}2^{-n} + \frac{1}{2}(1 - 2^{-2n}) = 1/2 + \underbrace{\frac{1}{2}(2^{-n} - 2^{-2n})}_{>0}$

Conclusion: This $\mathcal{D}$ has always a negligible, but non-zero advantage in distinguishing the PRG from a truly random source. Hence, if we had required that every $\mathcal{D}$ has zero advantage, then no PRG could exist w.r.t. this definition. (The proof given here of course only applies to PRGs of stretch $l(n) \geq 2n$, but the argument works similarly for $l(n) > n$ – at least it shows that "useful" PRGs cannot exist when requiring zero advantage.)

Exercise 2.4

(a) Show that PRFs with $l_{\text{out}}(n) \cdot 2^{l_{\text{in}}(n)} \leq n$ exist (unconditionally!).

(b) Let G be a PRG of stretch $l_G(n) = 2n$.

Split $G(k) =: G_0(k)||G_1(k)$ into two n bit strings.

Set $F_k^{(1)}(0) := G_0(k)$ and $F_k^{(1)}(1) := G_1(k)$. Show: $F^{(1)}$ is a PRF with $l_{\text{in}}(n) = 1$ and $l_{\text{out}}(n) = n$.

Solution:

(a) Since $l_{\text{out}}(n) \cdot 2^{l_{\text{in}}(n)} \leq n$ we can decompose any $k \in \{0,1\}^n$ into (at least) $N = 2^{l_{\text{in}}}$ parts k_i with $|k_i| = l_{\text{out}}$:

$$k = k_0||\cdots||k_{N-1}||\text{rest}$$

Set $F_k(\lfloor x \rceil) = k_x$. Then F_k is a truly random function as $k \overset{u}{\in} \{0,1\}^n$ and thus a PRF.

(b) i) Let $\mathcal{D}_F$ be a distinguisher for $F := F^{(1)}$.

We construct from it the distinguisher $\mathcal{D}_G$ for the underlying PRG G:

- Distinguisher $\mathcal{D}_G$ for G:
- ▷ Input: $y \in \{0,1\}^{2n}$
- ▷ Decompose y into $y_0||y_1 = y$ with $|y_0| = |y_1| = n$.
- ▷ $r \overset{r}{:=} \mathcal{D}_F^{\mathcal{O}}(1^n)$ where $\mathcal{D}_G$ simulates $\mathcal{O}$ as follows:
  - ▷ If $\mathcal{D}_F$ requires $\mathcal{O}(x)$ (for $x \in \{0,1\}$) give it y_x.
- ▷ return r

If $y \overset{u}{\in} \{0,1\}^{2n}$, then $\mathcal{D}_G$ simulates a RO; if $y \overset{r}{:=} G(x)$ for $x \overset{u}{\in} \{0,1\}^n$, then $\mathcal{D}_G$ simulates $F_k^{(1)}$. So, the probability for $\mathcal{D}_G$ to win in the PRG-Game is exactly the same as for D_F to win in the PRF-Game. As G is assumed to be a PRG, both probabilities are therefore negligible, so $F^{(1)}$ is indeed a PRF.