UCLouvain – EPL
LMAT2450: Cryptography
Year 2020-2021

Last Name: Peiffer
Given Name: Gilles
NOMA: 24321600

LMAT2450 – First Homework

Question 1: Pseudorandom Generator.

Let G be a pseudorandom generator (PRG) such that, if $s \in \{0,1\}^n$, then $G(s) \in \{0,1\}^{l(n)}$ with $l(n) > n$.

We define, for $s_1, s_2 \in \{0,1\}^n$, $G'(s_1||s_2) := G(s_1)||s_2$ where $G'(s_1||s_2) \in \{0,1\}^{l(n)+n}$.

Show that either G' is a PRG by offering a reduction to the security of G, or that G' is not a PRG by exhibiting an attack (building a distinguisher with non negligible advantage).

Solution: We show that G' is a PRG by reduction: any distinguisher D' for G' with probability of success $\eta(n)$ can be adapted to build a distinguisher D for G with the same probability of success, as follows:

- On input r, D will just simulate D' on $r\|r'$, for a randomly chosen $r' \in \{0,1\}^n$.
- If r is truly random, then so is $r\|r'$, whereas if $r = G(s)$ for a random $s \in \{0,1\}^n$, then $r\|r' = G(s)\|r' = G'(s\|r')$.

Formally, it holds that

$$\begin{aligned}
&\left| \Pr_{s\leftarrow\{0,1\}^n}\Big[D\big(G(s)\big)=1\Big] - \Pr_{r\leftarrow\{0,1\}^{\ell(n)}}\Big[D(r)=1\Big]\right| \\
=&\left| \Pr_{s\|r'\leftarrow\{0,1\}^{2n}}\Big[D'\big(G(s)\|r'\big)=1\Big] - \Pr_{r\|r'\leftarrow\{0,1\}^{\ell(n)+n}}\Big[D'(r\|r')=1\Big]\right| \\
=&\left| \Pr_{s\|r'\leftarrow\{0,1\}^{2n}}\Big[D'\big(G'(s\|r')\big)=1\Big] - \Pr_{r\|r'\leftarrow\{0,1\}^{\ell(n)+n}}\Big[D'(r\|r')=1\Big]\right| \\
=&\left| \Pr_{s'\leftarrow\{0,1\}^{2n}}\Big[D'\big(G'(s')\big)=1\Big] - \Pr_{r''\leftarrow\{0,1\}^{\ell(n)+n}}\Big[D'(r'')=1\Big]\right| \\
=&\,\eta(n).
\end{aligned}$$

Note the changes of subscripts for the probabilities. This shows that if we can distinguish G' with probability $\eta(n)$, we can also distinguish G with that same probability. By assumption, $\eta(n)$ must be negligible (as G is a PRG); we hence conclude that G' is a PRG too.

Question 2: Pseudorandom Function.

Consider F a pseudorandom function (PRF) such that $F : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^n$.

We define $F' : \{0,1\}^n \times \{0,1\}^{2n} \longrightarrow \{0,1\}^n$ such that $F'(k, x||y) := F(k,x) \oplus F(k,y)$.

Show either that F' is a PRF by providing a reduction to the security of F, or that F' is not a PRF by exhibiting an attack (building a distinguisher with non negligible advantage).

Solution: F' is not a PRF. We show it by building a distinguisher D which wins with non-negligible probability. D queries its oracle $\mathcal{O}$ for $\mathcal{O}(x\|x)$, for some value $x \in \{0,1\}^n$ (for simplicity, we take $x = 1^n$). If the output $\mathcal{O}(x\|x) = 0^n$, D outputs $b' = 1$, and otherwise it outputs $b' = 0$. The probability that a random function would give output 0^n for an input of the form $x\|x$ is 2^{-n}, whereas for F' this probability is 1.

Formally, we have (where $\mathsf{Func}_{2n,n}$ is the set of all functions mapping $2n$-bit strings to n-bit strings)

$$\left| \Pr_{k \leftarrow \{0,1\}^n} \left[D^{F'(k,\cdot)}(1^n) = 1 \right] - \Pr_{f \leftarrow \mathsf{Func}_{2n,n}} \left[D^{f(\cdot)}(1^n) \right] \right| = 1 - 2^{-n}.$$

This is clearly not negligible, and hence shows that F' is not a PRF.

Last Name: Peiffer
Given Name: Gilles
NOMA: 24321600

Question 3: How not to derive a PRG.

Let G be a PRG such that, if $s \in \{0,1\}^n$, then $G(s) \in \{0,1\}^{l(n)}$ with $l(n) > n$. Define also G' such that $G'(s) := G(s) \oplus (0^{l(n)-n}||s)$.

Show that G' may not be a PRG.

Solution: We show a scenario in which G' is not a PRG. Suppose G is such that the last bit of its output is always equal to the last bit of the input. In that case, the output of G' always has a zero last bit, which allows us to build a distinguisher D' with non-negligible chance of success: it predicts $b' = 1$ when the last bit of the output is zero, and $b' = 0$ otherwise. For a truly random generator, this would only be accurate half the time, but for the specification of the PRG we give it would always be right, meaning that it wins the distinguishing game with non-negligible probability:

$$\left| \Pr_{s \leftarrow \{0,1\}^n} \left[D'\big(G'(s)\big) = 1 \right] - \Pr_{r \leftarrow \{0,1\}^{\ell(n)}} \left[D'(r) = 1 \right] \right| = 1 - \frac{1}{2} = \frac{1}{2}.$$

It then remains to show that there exists a PRG G satisfying this property. Conveniently, the definition of G' from the first exercise of this homework satisfies this definition (if we rework it so as to have the right lengths).