Exercise Sheet 2

Nguyen Xuan Binh 887799

Aalto University, Finland

Exercise 1 (PRGs can leak half their input). Let $f : \{0,1\}^* \to \{0,1\}^*$ be a PRG. We define

$$g_f(x) = f(x_\ell)||x_r$$

Here, x_ℓ consists of the first $\lceil |x|/2 \rceil$ bits of x and x_r consists of the last $\lfloor |x|/2 \rfloor$ bits of x, i.e., $x = x_\ell||x_r$.

Task: Prove via reduction that if f is a PRG, then g_f is a PRG, too.

— **Base case**: $|x| = 1$

When $|x| = 1$, then $x_\ell = x_1$ and $x_r = x_{empty}$. In other words, x_ℓ is the one bit and x_r is empty. Applying the PRG g_f to x, we have:

$$g_f(x) = f(x_1),$$

which is a PRG because f is a PRG and the output of g_f is completely derived from f. Therefore, the base case of the proof is correct. Additionally, it follows that the first bit cannot be a hardcore bit, since, if the function leaks its first half, then it also leaks the first bit, so, given $f(x)$, the first bit of x would then be easy to distinguish. A same analysis applies to any input bit. Therefore, we assume that at the base case, the first bit is not hardcore bit, but it has already become pseudorandom thanks to $f(x)$. Any other bits thus can be hardcore bit

— **Induction steps**:

Assume that $g_f(x)$ is a PRG at the stage $|x| = \lambda$, or x_r is PRG. We need to prove that $g_f(x)$ is also a PRG at the stage $|x| = \lambda + 1$, or x_r is still PRG. There are two distinct cases, which are odd and even values of λ.

- When λ is even, then $x_\ell = x_{1\to\frac{\lambda}{2}}$ and $x_r = x_{\frac{\lambda}{2}+1\to\lambda}$. The size of x_ℓ is then the first $\frac{\lambda}{2}$ bits and the size of x_r is the last $\frac{\lambda}{2}$ bits. In the next induction step, $x_\ell = x_{1\to\frac{\lambda}{2}+1}$ and $x_r = x_{\frac{\lambda}{2}+2\to\lambda+1}$. The size of x_ℓ is then the first $\frac{\lambda}{2} + 1$ bits and the size of x_r is the last $\frac{\lambda}{2}$ bits. Since the added bit in the next step belongs to x_ℓ, it will be generated by f and is still PRG. Because x_r is unchanged in the next step and is assumed to be PRG, it means that g_f is PRG as well when $|x| = \lambda + 1$.
- When λ is odd, then $x_\ell = x_{1\to\frac{\lambda+1}{2}}$ and $x_r = x_{\frac{\lambda+1}{2}+1\to\lambda}$. The size of x_ℓ is then the first $\frac{\lambda+1}{2}$ bits and the size of x_r is the last $\frac{\lambda+1}{2} - 1$ bits. In the next induction step, $x_\ell = x_{1\to\frac{\lambda+1}{2}}$ and $x_r = x_{\frac{\lambda+1}{2}+2\to\lambda+1}$. The size of x_ℓ is then the first $\frac{\lambda+1}{2}$ bits and the size of x_r is the last $\frac{\lambda+1}{2}$ bits. In this case, the introduced bit is added to x_r. Since at the base case, the hardcore bit should not be the first bit but can be any other bit, we can regard this new leaked bit added to x_r as the hardcore bit. Since x_r is stretched by $s(n) = 1$ by a hardcore bit, x_r at the next induction step is still PRG because x_r is assumed to be PRG at the current step. Since g_f is PRG at the next induction step for both odd and even λ and g_f is also PRG at the base case, it is true that g_f is actually a PRG (proven).

Exercise 2 (Some OWFs are not PRGs)**.** Assume the existence of length-preserving one-way functions.

Task: Show that there exists a length-expanding one-way function h which is not a PRG.

First of all, we call this length-preserving OWF as $f(x)$ and the length-expanding OWF as h(x), with the stretch $s(n) = \lambda$. Because $f(x)$ is OWF, it must also be a PRG according to the Hill's Theorem. We can prove the existence of h(x) such that it is not a PRG as follows:

$$h(x) := f(x)||0^{\lambda}$$

This basically means that $h(x)$ is $f(x)$ concatenated with 0s of size λ. Because $f(x)$ is OWF, appending zeros or any constant array of bits to any image of x via $f(x)$ also results in a unique output, making $h(x)$ an OWF. However, $h(x)$ is definitely not a PRG, because of the deterministic constant 0s appending at the end, making the output not random anymore. For example, consider an adversary $\mathcal{A}$ that tries to determine whether $h(x)$ is ideal or real PRG. Due to the consistent 0s left appending, $\mathcal{A}$ can be sure that the OWF is not an ideal PRG, as they can input any preimage to $h(x)$ and receive the same last number of 0 bits. Therefore, there exists a length-expanding OWF such that it is not a PRG (proven).