CS-E4340 Cryptography: Exercise Sheet 3

Submission Deadline: September 26, 11:30 via MyCourses

Each exercise can give up to two participation points, 2 for a mostly correct solution and 1 point for a good attempt. Overall, the exercise sheet gives at most 4 participation points.

Exercise Sheet 3 is intended to help...

(a) ...understand the definition of pseudorandom functions (PRFs).
(b) ...understand the difference between a PRF and a pseudorandom generator (PRG), which we considered before.
(c) ...familiarize yourself with the notion of a reduction (continued).
(d) ...familiarize yourself with the notion of a negligible function.

Exercise 1 shows PRFs *do* hide their input unlike some other primitives we saw thus far.
Ex. 2 & Ex. 3 concern properties of PRFs and PRGs.
Exercise 2 shows that the existence of PRFs implies the existence of PRGs.
Exercise 3 shows how a quadratic key PRF and PRG can be used to obtain a standard PRF.
Exercise 4 is intended to help with the notions of negligible functions and why they are a convenient notion of a "small" function.

Exercise 1 (**PRFs hide their input**). Let f be a (λ, λ)-PRF, and consider the following transformations:

(a) $h_1(k, x) := f(k, 0||x_{2..|x|})$.
(b) $h_2(k, x) := x_1||f(k, x)_{2..|x|}$.

Task: Show that h_1 and h_2 are not PRFs (even though f is a PRF).
Hint: Find an efficient adversary $\mathcal{A}$ such that $\mathbf{Adv}^{\mathsf{PRF}}_{h,\mathcal{A}}(1^\lambda)$ is non-negligible. (In fact, we can even give an adversary which has advantage almost 1, but this is not required to solve this exercise.)

Solution 1. Consider the following adversaries $\mathcal{A}_1$ and $\mathcal{A}_2$ against $\texttt{Gprf}_{h_1}$ and $\texttt{Gprf}_{h_2}$, respectively:

$\mathcal{A}_1(1^\lambda)$	$\mathcal{A}_2(1^\lambda)$
$y \leftarrow \mathsf{EVAL}(0^\lambda)$	$y \leftarrow \mathsf{EVAL}(0^\lambda)$
$y' \leftarrow \mathsf{EVAL}(1\|\|0^{\lambda-1})$	**return** y_1
return $y = y'$	

Polynomial time: Since oracle queries count only one step, both $\mathcal{A}_1$ and $\mathcal{A}_2$, the oracle queries only add one step to the runtime of $\mathcal{A}_1$ and $\mathcal{A}_2$. Other parts of the runtime of $\mathcal{A}_1$ and $\mathcal{A}_2$ is writing one or two λ-bit strings (which takes time linear in λ) and, in the case of $\mathcal{A}_1$, comparing two λ-bit strings (which also takes time linear in λ). Thus, the runtime of both $\mathcal{A}_1$ and $\mathcal{A}_2$ is linear in λ.
Probability analysis: We need to show that the advantage

$$\mathsf{Adv}^{\mathsf{Gprf}}_{h_j,\mathcal{A}_j}(\lambda) := \left|\Pr\left[1 = \mathcal{A}_j \to \texttt{Gprf}^0_{h_j}\right] - \Pr\left[1 = \mathcal{A}_j \to \texttt{Gprf}^1\right]\right|$$

is non-negligible for $j \in \{1, 2\}$. To do so, let us first analyse the real games $\texttt{Gprf}^0_{h_j}$ and then ideal games $\texttt{Gprf}^1$.
In the real game $\texttt{Gprf}^0_{h_j}$ $\mathsf{PRF}(x, \lambda) = h_j(k, x)$, where k is the key stored in the $\texttt{Key}$-package. By definition of h_1 and h_2, we have

$$\begin{aligned} h_1(k, 0^\lambda) &= f(k, 0||0^{\lambda-1}) \\ h_1(k, 1||0^{\lambda-1}) &= f(k, 0||0^{\lambda-1}) \\ h_2(k, 0^\lambda) &= 0||f(k, 0^\lambda)_{2\ldots\lambda} \end{aligned}$$

Therefore, the values of $h_1(k, 0^\lambda)$ and $h_1(k, 1||0^{\lambda-1})$ always agree, and the first bit of $h_2(k, 0^\lambda)$ is always 0. As the comparison and first bit are the outputs of $\mathcal{A}_1 \to \texttt{PRF}^0_{h_1}(1^\lambda)$ and $\mathcal{A}_2 \to \texttt{PRF}^0_{h_2}(1^\lambda)$, respectively, we therefore have

$$\begin{aligned} \Pr\left[1 = \mathcal{A}_1 \to \texttt{Gprf}^0_{h_1}\right] &= 1 \\ \Pr\left[1 = \mathcal{A}_2 \to \texttt{Gprf}^0_{h_2}\right] &= 0. \end{aligned}$$

In the ideal game $\texttt{Gprf}^1$, the first time $\mathsf{PRF}(x, \lambda)$ is called for any new input x, it returns a uniformly random bit-string of length λ. In other words, all assignments in $\mathcal{A}_j \to \texttt{Gprf}^1$ are equivalent to sampling a uniformly random $z \leftarrow\!\!\$ \{0,1\}^\lambda$. The first adversary $\mathcal{A}_1$ then compares two uniformly random values, which agree with probability $2^{-\lambda}$ and $\mathcal{A}_2$ returns one bit of y, which has equal probability to be 0 or 1. Therefore, we have

$$\begin{aligned} \Pr\left[1 = \mathcal{A}_1 \to \texttt{Gprf}^1\right] &= \frac{1}{2^\lambda} \\ \Pr\left[1 = \mathcal{A}_2 \to \texttt{Gprf}^1\right] &= \frac{1}{2}. \end{aligned}$$

Substituting our computations into advantage thus yields

$$\begin{aligned}\mathsf{Adv}^{\mathsf{Gprf}}_{h_j,\mathcal{A}_j}(\lambda) &:= \left|\Pr\left[1 = \mathcal{A}_j \to \texttt{Gprf}^0_{h_j}\right] - \Pr\left[1 = \mathcal{A}_j \to \texttt{Gprf}^1\right]\right| \\ &= \begin{cases}\left|1 - 2^{-\lambda}\right|, & \text{if } j = 1 \\ \left|0 - \frac{1}{2}\right|, & \text{if } j = 2\end{cases}\end{aligned}$$

which are both clearly non-negligible, thus the functions are not pseudorandom functions.

Exercise 2 (PRFs imply PRGs). Let f be a PRF. Define

$$G(z) := f(z, 0^{|z|})||f(z, 1^{|z|}).$$

Task: Prove via reduction, that G is a PRG with output length $|G(z)| = 2|z|$.

Solution 2. Firstly, note that for all $z \in \{0,1\}^*$, we have that $|G(z)| = \left|f(z, 0^{|z|})\right| + \left|f(z, 1^{|z|})\right| = 2|z|$ where the latter equation follows from the length-requirement of the PRF. Secondly, note that G is polynomial-time computable, since f is polynomial-time computable and as G essentially consists of 2 evaluations of f.
We now turn to proving the pseudorandomness property of G. Assume towards contradiction that G is not a PRG and that there exists an efficient distinguisher $\mathcal{A}$ for G. We build a reduction $\mathcal{R}_{\mathcal{A}}$ as follows:

$$\begin{array}{l}\underline{\mathcal{R}_{\mathcal{A}}(1^\lambda)} \\ y \leftarrow \mathsf{EVAL}(0^\lambda)||\mathsf{EVAL}(1^\lambda) \\ x \leftarrow\!\!\$\; \mathcal{A}(y, 1^\lambda) \\ \textbf{return } x\end{array}$$

Polynomial time: To see that the reduction $\mathcal{R}$ runs in polynomial-time, note that oracle queries only count one step.
Probability Analysis: We will show that

$$\mathsf{Adv}^{\mathsf{Gprf}}_{f,\mathcal{R}_{\mathcal{A}}}(\lambda) := \left|\Pr\left[1 = \mathcal{R}_{\mathcal{A}} \to \texttt{Gprf}^0_f\right] - \Pr\left[1 = \mathcal{R}_{\mathcal{A}} \to \texttt{Gprf}^1\right]\right|$$

is equal to

$$\begin{aligned}\mathsf{Adv}^{\mathsf{PRG}}_{G,\mathcal{A}}(\lambda) &:= |\Pr\left[\mathsf{Exp}^{\mathsf{PRG},0}_{G,s,\mathcal{A}}(1^\lambda) = 1\right] - \Pr\left[\mathsf{Exp}^{\mathsf{PRG},1}_{s,\mathcal{A}}(1^\lambda) = 1\right]| \\ &= |\Pr_{z \leftarrow\$\{0,1\}^\lambda}\left[\mathcal{A}(G(z), 1^\lambda) = 1\right] - \Pr_{y \leftarrow\$\{0,1\}^{2\lambda}}\left[\mathcal{A}(y, 1^\lambda) = 1\right]|\end{aligned}$$

Thus, if $\mathsf{Adv}^{\mathsf{PRG}}_{G,\mathcal{A}}$ is non-negligible, then $\mathsf{Adv}^{\mathsf{Gprf}}_{f,\mathcal{R}_{\mathcal{A}}}$ is non-negligible, too.
We observe that in the real PRF game

$$\Pr\left[1 = \mathcal{R}_{\mathcal{A}} \to \texttt{Gprf}^0_f\right] = \Pr_{z \leftarrow\$\{0,1\}^\lambda}\left[\mathcal{A}(f(z, 0^\lambda)||f(z, 1^n), 1^\lambda) = 1\right]$$

by definition of the reduction $\mathcal{R}_{\mathcal{A}}$, which is equal to $\Pr_{z \leftarrow\$\{0,1\}^\lambda}\left[\mathcal{A}(G(z), 1^\lambda) = 1\right]$ by definition of G.
Moreover, in the ideal game

$$\Pr\left[1 = \mathcal{R}_{\mathcal{A}} \to \texttt{Gprf}^1\right] = \Pr_{y_\ell \leftarrow\$\{0,1\}^\lambda, y_r \leftarrow\$\{0,1\}^\lambda}\left[\mathcal{A}(y_\ell||y_r, 1^\lambda) = 1\right]$$

by definition of $\mathcal{R}_\mathcal{A}$. Now, this term is equal to $\Pr_{y \leftarrow \$ \{0,1\}^{2\lambda}}\left[\mathcal{A}(y, 1^\lambda) = 1\right]$ by sampling both parts y_ℓ and y_r together instead of separately. As the probabilities are equal, this implies

$$\mathsf{Adv}^{\mathsf{Gprf}}_{f,\mathcal{R}_\mathcal{A}}(\lambda) = \mathsf{Adv}^{\mathsf{PRG}}_{G,\mathcal{A}}(\lambda),$$

which is assumed non-negligible, contradicting the pseudo-randomness of f. Thus G is a PRG.

Exercise 3. (Key Expansion) A *quadratic-key* (λ, λ)-PRF f_q is a PRF which maps a key k of length λ^2, and an input x of length λ to an output y of length λ. Let f_q be a quadratic-key PRF. Let G be a PRG with $|G(z)| = |z|^2$. Define

$$f(k, x) := f_q(G(k), x)$$

Task: Show that f is a (standard) PRF.
Hint: Given a successful distinguisher for the PRF f, show that one of the following is true: (i) There exists a successful distinguisher for the PRG G or (ii) there exists a successful distinguisher for the quadradic-key PRF f_q.

Solution 3. Before carrying out the actual proof, let us discuss the high-level idea of the proof. The idea is to first replace $G(k)$ with a random string of equal length and to reduce to the PRG security of G. In the next step, one can then reduce to the PRF security of f. We now make this argument rigorous.

Claim. If G is a PRG with $|G(z)| = |z|^2$ and f_q is a quadratic key PRF, then $f(k, x) := f_q(G(k), x)$ is a PRF.

The proof consists of two steps. The first is to establish that $f_q(G(U(1^\lambda)), \cdot)$ is indistinguishable from $f_q(U(1^{\lambda^2}), \cdot)$, where $U(1^\lambda)$ denotes a uniformly random bitstring of length λ (PRG-security of G). The second step is then to show that $f_q(U(1^{\lambda^2}), \cdot)$ is indistinguishable from a truly random function.

Step 1. We begin by reducing the indistinguishability of $f_q(G(U(1^\lambda)), x)$ and $f_q(U(1^{\lambda^2}), \cdot)$ to the PRG security of G. Thus we assume towards contradiction that there exists a PPT distinguisher $\mathcal{A}$ such that

$$\begin{aligned}\mathsf{Adv}^{\mathsf{PRG}}_{f_q(G,\cdot),\mathcal{A}}(\lambda) := \big| &\Pr_{k \leftarrow \$ \{0,1\}^\lambda}\left[\mathcal{A}(f_q(G(k), \cdot), 1^\lambda)) = 1\right] \\ &- \Pr_{z \leftarrow \$ \{0,1\}^{\lambda^2}}\left[\mathcal{A}(f_q(z, \cdot), 1^\lambda)) = 1\right]\big|\end{aligned}$$

is non-negligible. We build our reduction as follows:

$$\begin{array}{l}\underline{\mathcal{R}_\mathcal{A}(y, 1^{|y|})} \\ b \leftarrow \mathcal{A}(f_q(y, \cdot), 1^{|y|}) \\ \textbf{return } b\end{array}$$

where $\cdot$ denotes some arbitrary query.
Polynomial time: Since $\mathcal{A}$ is a polynomial-time adversary, $\mathcal{R}_\mathcal{A}$ also runs in polynomial time.
Probability Analysis: We need to show that the PRG advantage

$$\mathsf{Adv}^{\mathsf{PRG}}_{G,\mathcal{R}_\mathcal{A}}(\lambda) := \left|\Pr_{k \leftarrow \$ \{0,1\}^\lambda}\left[\mathcal{R}_\mathcal{A}(G(k), 1^\lambda) = 1\right] - \Pr_{z \leftarrow \$ \{0,1\}^{\lambda^2}}\left[\mathcal{R}_\mathcal{A}(z, 1^\lambda) = 1\right]\right|$$

is non-negligible. The reduction $\mathcal{R}_\mathcal{A}$ receives input z, calls the distinguisher $\mathcal{A}$ and returns 1 if and only if $\mathcal{A}$ returns 1, we get that

$$\begin{aligned}\mathsf{Adv}^{\mathsf{PRG}}_{G,\mathcal{R}_\mathcal{A}}(\lambda) &:= \left|\Pr_{k \leftarrow \$\{0,1\}^\lambda}\left[\mathcal{A}(f_q(G(k),\cdot),1^\lambda)=1\right] - \Pr_{z \leftarrow \$\{0,1\}^{\lambda^2}}\left[\mathcal{A}(f_q(z,\cdot),1^\lambda)=1\right]\right| \\ &= \mathsf{Adv}^{\mathsf{PRG}}_{f_q(G,\cdot),\mathcal{A}}(\lambda),\end{aligned}$$

which is non-negligible by our assumption, contradicting the PRG security of G.

Step 2. We will next use the result from step 1, as well as the PRF-security of f_q to prove the PRF-security of f. PRF-security of f_q gives us that for all adversaries $\mathcal{A}$, we have that

$$\mathsf{Adv}^{\mathsf{PRF}}_{f_q,\mathcal{A}}(\lambda) := \left|\Pr\left[1 = \mathcal{A} \to \mathtt{Gprf}^0_{f_q}\right] - \Pr\left[1 = \mathcal{A} \to \mathtt{Gprf}^1\right]\right|$$

is negligible. Through step 1, we know that

$$\begin{aligned}\mathsf{Adv}^{\mathsf{PRG}}_{f_q(G,\cdot),\mathcal{A}}(\lambda) := \Big|&\Pr_{k \leftarrow \$\{0,1\}^\lambda}\left[\mathcal{A}(f_q(G(k),\cdot),1^\lambda))=1\right] \\ &- \Pr_{z \leftarrow \$\{0,1\}^{\lambda^2}}\left[\mathcal{A}(f_q(z,\cdot),1^\lambda))=1\right]\Big|\end{aligned}$$

is also negligible. Finally, we want to prove that

$$\mathsf{Adv}^{\mathsf{PRF}}_{f,\mathcal{A}}(\lambda) := \left|\Pr\left[1 = \mathcal{A} \to \mathtt{Gprf}^0_{f}\right] - \Pr\left[1 = \mathcal{A} \to \mathtt{Gprf}^1\right]\right|$$

is negligible. With the PRG security of G and PRF security of f_q and the triangle inequality, we can obtain the upper bound

$$\mathsf{Adv}^{\mathsf{PRF}}_{f,\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{PRG}}_{f_q(G,\cdot),\mathcal{R}_\mathcal{A}}(\lambda) + \mathsf{Adv}^{\mathsf{PRF}}_{f_q,\mathcal{A}}(\lambda).$$

Thus we have a negligible upper bound on the advantage of any adversary $\mathcal{A}$ against the PRF-security of f.

Exercise 4 (**Negligible Functions**)**.** Recall the definition of negligible functions.

Definition 1 A function $\nu : \mathbb{N} \to \mathbb{R}^+_0$ is *negligible* if for all constants c there exists a natural number $N \in \mathbb{N}$ such that for all $n > N$ it holds that $\nu(n) < \frac{1}{n^c}$.

Closer to the verbal description of negligible function given in the lecture notes for lecture 3, we may like to define negligible functions as follows:

Definition 1' A function $\nu : \mathbb{N} \to \mathbb{R}^+_0$ is *negligible* if for all positive polynomials p there exists a natural number $N \in \mathbb{N}$ such that for all $n > N$ it holds that $\nu(n) < \frac{1}{p(n)}$.

Prove at least two out of (a), (b) and (c):

(a) Definitions 1 and 1' of negligible functions are equivalent.

(b) The following are true:

(i) The sum of two negligible functions is negligible.

(ii) Multiplying a negligible function by an (arbitrary) positive polynomial yields a negligible function.

Hint: You may use either of the two definitions in your proof.

(c) (Challenging) There exists a sequence of negligible functions $\nu_\lambda : \mathbb{N} \to [0,1]$ such that the function $\mu(\lambda) := \sum_{i=1}^{\lambda} \nu_i(\lambda)$ is the constant 1 function, i.e., for all $\lambda \in \mathbb{N}$, it holds that $\mu(\lambda) = 1$.
Hint: Use diagonalization.

Solution 4. (a) To prove that the definitions are equivalent, we need to show that if a function ν is negligible according to one of the definitions, then it is also negligible according to the other definition. We will prove implications in both directions separately.

$\boxed{\textbf{1'} \implies \textbf{1}}$ Assume a function $\nu : \mathbb{N} \to \mathbb{N}$ is negligible according to definition 1'. Take a positive constant c, and let $d = \lceil c \rceil$. Consider the polynomial $p(n) = n^d$. By definition 1', there exists $N \in \mathbb{N}$ such that $\nu(n) < \frac{1}{p(n)}$ for all $n > N$. Since $d \geq c$, it holds that $\frac{1}{n^d} \leq \frac{1}{n^c}$ for all $n \in \mathbb{N}$. In particular, for $n > N$ this thus implies that $\nu(n) < \frac{1}{n^c}$. Since c was an arbitrary positive constant, ν is also negligible according to definition 1.

$\boxed{\textbf{1} \implies \textbf{1'}}$ Assume a function $\nu : \mathbb{N} \to \mathbb{N}$ is negligible according to definition 1'. Let $p(n) = a_d n^d + a_{d-1} n^{d-1} + \cdots + a_1 n + a_0$ be an arbitrary positive polynomial of order d. Let $a = |a_d| + |a_{d-1}| + \cdots + |a_0|$, so that $p(n) \leq an^d$ for every $n \in \mathbb{N}$. If we choose c large enough such that $a \cdot 2^d \leq 2^c$, then $an^d \leq n^c$ for all $n \geq 2$. By definition 1' there exists $N \in \mathbb{N}$ such that for every $n > N$ it holds that $\nu(n) < \frac{1}{n^c}$. As we saw before, it also holds that $\frac{1}{n^c} \leq \frac{1}{an^d} \leq \frac{1}{p(n)}$, therefore also $\nu(n) < \frac{1}{p(n)}$ for $n > N$. As p was an arbitrary positive polynomial, it follows that ν is negligible also according to definition $1'$.

(b) To prove (i) and (ii), we use the definition 1' of negligible functions:

(i) Let ν and μ be negligible. We want to show that their sum $\eta := \nu + \mu$ is also negligible.
Let p be a positive polynomial. Then also $2p$ is a positive polynomial. Since ν and μ are negligible, there exists $N \in \mathbb{N}$ such that $\nu(n) < \frac{1}{2p(n)}$ and $\mu(n) < \frac{1}{2p(n)}$ for every $n > N$. Therefore, we get

$$\eta(n) = \nu(n) + \mu(n) < \frac{1}{2p(n)} + \frac{1}{2p(n)} = \frac{1}{p(n)}.$$

Since the polynomial p was arbitrary, this proves that η is negligible by definition 1'.

(ii) Let ν be negligible and q be a polynomial. We want to show that their product $\eta = q\nu$ is negligible. Suppose, for contradiction that η is not negligible. Now there exists a positive polynomial p such that for all $N \in \mathbb{N}$ there is $n > N$ such that $\eta(n) \geq \frac{1}{p(n)}$. That is

$$\nu(n)q(n) \geq \frac{1}{p(n)} \quad \Big| \text{ if } q \text{ is negative or 0, we have a contradiction. Suppose } q > 0.$$
$$\nu(n) \geq \frac{1}{p(n)q(n)}$$

where $p(n)q(n)$ is some positive polynomial. However, the last inequality is a contradiction since ν is negligible. So η has to be negligible.

(c) Choose

$$\nu_i(n) = \begin{cases} 1 & \text{if } n = i \\ 0 & \text{otherwise} \end{cases}$$

for all $i \in \mathbb{N}$. Now all such ν_i are negligible, since for all $n > i$, the function $\nu_i(n)$ is 0 which is clearly less than any inverse positive polynomial.
Now

$$\begin{aligned}\mu(\lambda) &= \sum_{i=1}^{\lambda} \nu_i(\lambda) \\ &= 0 + 0 + ... + 0 + \nu_\lambda(\lambda) \\ &= 0 + 0 + ... + 0 + 1 \\ &= 1\end{aligned}$$

which proves the statement.
Take home: sum of constant number of negligible functions is negligible, but unbounded sum of negligible functions is not always negligible. Careful with infinities!