zu Aufgabe 3.1

Nachfolgend sind einige „Familien“ von Abbildungen beschrieben, nämlich jeweils zu jedem $K \in \mathcal{K} = \{0,1\}^k$ eine Abbildung $E_K\colon \{0,1\}^\ell \to \{0,1\}^\ell$. Welche dieser Familien sind PRF-sicher, welche nicht?

Bei Sicherheit ist hier kein Beweis verlangt.

Geben Sie bei Unsicherheit einen erfolgreichen PRF-Angreifer an! Das muss nicht der bestmögliche Angreifer sein.

Hinweise: PRF-Unsicherheit bedeutet, es gibt einen erfolgreichen PRF-Angreifer – also einen Angreifer mit einem PRF-Vorteil, der nicht verschwindend gering ist. Der Vorteil kann aber näher an der 0 liegen als an der 1. Auf die Laufzeit des Angriffs kommt es hier nicht an.

a. $k = 1, \ell = 1$

	$E_K(0)$	$E_K(1)$
$K = 0$	0	1
$K = 1$	1	0

Diese Familie von Abbildungen ist nicht PRF-sicher.

Ein PRF-Angreifer hat Zugriff auf ein Orakel $E(\cdot)$, das je nach Fall des Angriffsspiels die Orakelanfragen immer entweder mit den entsprechenden Werten von $E_K(\cdot)$ für ein $K \in_\$ \mathcal{K}$ beantwortet oder mit den entsprechenden Werten von $f(\cdot)$ für ein $f \in_\$ \mathrm{Func}(\{0,1\}^\ell)$. Die Aufgabe des Angreifers ist es, zu erkennen, ob vermutlich der Fall mit einem solchen $E_K(\cdot)$ vorliegt oder der Fall mit einem solchen $f(\cdot)$. Wir können einen Angreifer $\boldsymbol{A}$ hier z. B. wie folgt konstruieren:

- $\boldsymbol{A}$ stellt an sein Orakel zunächst die Anfrage 0 und erhält eine Anwort $E(0)$, dann die Anfrage 1 und erhält eine Antwort $E(1)$.
- Gilt nun entweder $E(0) = 0 \wedge E(1) = 1$ oder $E(0) = 1 \wedge E(1) = 0$, so gibt $\boldsymbol{A}$ das Bit 1 aus; andernfalls das Bit 0.

Dieser Angreifer gibt also genau dann das Bit 1 aus und rät damit, dass er es mit $E_K(\cdot)$ zu tun hatte, wenn das Verhalten von $E(\cdot)$ zu $E_0(\cdot)$ oder zu $E_1(\cdot)$ aus der Aufgabenstellung passt. Dass wir so tatsächlich einen erfolgreichen Angreifer beschrieben haben, sehen wir in Aufgabe 3.2 a.

b. $k = 2, \ell = 1$

	$E_K(0)$	$E_K(1)$
$K = 00$	1	0
$K = 01$	0	0
$K = 10$	0	1
$K = 11$	1	1

Diese Familie ist PRF-sicher!

Zum Beweis (in der Aufgabe nicht verlangt) stellt man fest, dass es sich bei den vier Abbildungen $E_K(\cdot)$ laut Tabelle ($K \in \{00, 01, 10, 11\}$) gerade um alle vier Abbildungen in

Func($\{0,1\}$) handelt. Jeder Angreifer $\boldsymbol{A}$ erlebt also im Angriffsspiel auch bei Interaktion mit $E_K(\cdot)$ mit Wahrscheinlichkeit jeweils $\frac{1}{4}$ jede Abbildung aus Func($\{0,1\}$), somit gilt

$$\Pr_{K\in_\$\mathcal{K}}\left[\boldsymbol{A}^{E_K(\cdot)} \Rightarrow 1\right] \;=\; \Pr_{f\in_\$\mathrm{Func}(\{0,1\})}\left[\boldsymbol{A}^{f(\cdot)} \Rightarrow 1\right],$$

ganz egal, wie der Angreifer vorgeht. Es folgt $\mathrm{Adv}^{\mathrm{PRF}}_{E_K,\boldsymbol{A}} = 0$.

c. $k = 2, \ell = 1$

	$E_K(0)$	$E_K(1)$
$K = 00$	1	1
$K = 01$	0	1
$K = 10$	1	0
$K = 11$	0	1

Bei der Definition von E_K hier fällt auf, dass es zwei Zeilen gibt mit $E_K(0) = 0 \wedge E_K(1) = 1$; dafür fehlt eine Zeile mit $E_K(0) = 0 \wedge E_K(1) = 0$ völlig. Das führt zur Vermutung, dass E_K nicht PRF-sicher ist. Ein Angreifer $\boldsymbol{A}$ kann z. B. wie folgt vorgehen:

- $\boldsymbol{A}$ stellt an sein Orakel zunächst die Anfrage 0 und erhält eine Anwort $E(0)$, dann die Anfrage 1 und erhält eine Antwort $E(1)$.
- Gilt nun $E(0) = 0 \wedge E(1) = 1$, so gibt $\boldsymbol{A}$ das Bit 1 aus, andernfalls 0.

Zum Vorteil dieses Angreifers siehe Aufgabe 3.2 c.

d. $k = 2, \ell = 2$

	$E_K(00)$	$E_K(01)$	$E_K(10)$	$E_K(11)$
$K = 00$	00	01	10	11
$K = 01$	01	10	11	00
$K = 10$	10	11	00	01
$K = 11$	11	00	01	10

Hier fällt auf: Liest man die Zwei-Bit-Wörter als Binärzahlen ($00 = 0$, $01 = 1$, $10 = 2$, $11 = 3$), so gilt

$$E_K(m) = m + K \bmod 4$$

(z. B. $E_{10}(11) = 3 + 2 \bmod 4 = 01$). Wir vermuten, dass E_K nicht PRF-sicher ist. Ein Angreifer $\boldsymbol{A}$ kann etwa so vorgehen:

- $\boldsymbol{A}$ stellt an sein Orakel die Anfrage 00 und erhält eine Anwort $E(00)$, dann die Anfrage 01 mit Antwort $E(01)$.
- Gilt nun $E(00) + 1 \equiv E(01) \pmod 4$, so gibt $\boldsymbol{A}$ das Bit 1 aus, andernfalls 0.

Dieser Angreifer gibt also genau dann 1 aus und setzt so darauf, dass hinter dem Orakel die Abbildung $E_K(\cdot)$ steckt mit zufälligem K, wenn beide Antworten zum gleichen E_K passen – wenn es nämlich ein K gibt mit $E(00) = 00 + K \bmod 4$ und $E(01) = 01 + K \bmod 4$. Zum Vorteil dieses Angreifers siehe Aufgabe 3.2 d.

zu Aufgabe 3.2

Soweit Sie in Aufgabe 3.1 PRF-Unsicherheit festgestellt und dazu Angreifer beschrieben haben, geben Sie jeweils den PRF-Vorteil an!

Die folgenden Antworten gelten für diejenigen Angreifer, die oben (zu Aufgabe 3.1) beschrieben sind. Mit anderen Angreifern können sich andere PRF-Vorteile ergeben.

a. Zunächst sehen wir $\Pr_{K\in_\$\mathcal{K}}\left[\boldsymbol{A}^{E_K(\cdot)} \Rightarrow 1\right] = 1$, denn bei der Interaktion sowohl mit $E_0(\cdot)$ als auch mit $E_1(\cdot)$ gibt der oben (zu Aufgabe 3.1 a) beschriebene Angreifer $\boldsymbol{A}$ stets das Ergebnis 1 aus.

   Dagegen ist $\Pr_{f\in_\$\mathrm{Func}(\{0,1\})}\left[\boldsymbol{A}^{f(\cdot)} \Rightarrow 1\right] = \frac{1}{2}$. Das können wir sehen, indem wir alle vier Abbildungen aus $\mathrm{Func}(\{0,1\}$ tabellieren – nennen wir sie f_1, f_2, f_3 und f_4 – und jeweils überprüfen, welcher Ausgabewert von $\boldsymbol{A}$ sich ergibt:

$f = \ldots$	$f(0)$	$f(1)$	$\boldsymbol{A}^{f(\cdot)} \Rightarrow \ldots$
f_1	0	0	0
f_2	0	1	1
f_3	1	0	1
f_4	1	1	0

   Genau in zwei der vier Fälle gibt $\boldsymbol{A}$ das Bit 1 aus, so ergibt sich die Wahrscheinlichkeit von $\frac{2}{4} = \frac{1}{2}$.

   Zusammen ergibt sich

$$\mathrm{Adv}^{\mathsf{PRF}}_{E_K,\boldsymbol{A}} \;=\; \Pr_{K\in_\$\mathcal{K}}\left[\boldsymbol{A}^{E_K(\cdot)} \Rightarrow 1\right] - \Pr_{f\in_\$\mathrm{Func}(\{0,1\})}\left[\boldsymbol{A}^{f(\cdot)} \Rightarrow 1\right] \;=\; \frac{1}{2}.$$

c. Hier gilt $\Pr_{K\in_\$\mathcal{K}}\left[\boldsymbol{A}^{E_K(\cdot)} \Rightarrow 1\right] = \frac{1}{2}$, denn tabellieren wir zu jedem möglichen $K \in \mathcal{K}$ und den dazugehörigen Werten von $E_K(\cdot)$ den entsprechenden Ausgabewert von $\boldsymbol{A}$ (laut unserer Beschreibung eines $\boldsymbol{A}$ oben, zu Aufgabe 3.1 c), so ergibt sich das folgende Bild:

	$E_K(0)$	$E_K(1)$	$\boldsymbol{A}^{E_K(\cdot)} \Rightarrow \ldots$
$K = 00$	1	1	0
$K = 01$	0	1	1
$K = 10$	1	0	0
$K = 11$	0	1	1

   In zwei von vier möglichen Fällen ist die Ausgabe 1, deshalb die Wahrscheinlichkeit von $\frac{2}{4} = \frac{1}{2}$.

   Andererseits ist $\Pr_{f\in_\$\mathrm{Func}(\{0,1\})}\left[\boldsymbol{A}^{f(\cdot)} \Rightarrow 1\right] = \frac{1}{4}$. Das sehen wir durch Tabellieren der möglichen Abbildungen f_1, f_2, f_3 und f_4 mit den zugehörigen Ausgabewerten von $\boldsymbol{A}$:

$f = \ldots$	$f(0)$	$f(1)$	$\boldsymbol{A}^{f(\cdot)} \Rightarrow \ldots$
f_1	0	0	0
f_2	0	1	1
f_3	1	0	0
f_4	1	1	0

Nur in einem von vier Fällen wird 1 ausgegeben, deshalb die Wahrscheinlichkeit $\frac{1}{4}$.

Aus den Wahrscheinlichkeiten ergibt sich der Vorteil $\mathrm{Adv}^{\mathsf{PRF}}_{E_K,\boldsymbol{A}} = \frac{1}{2} - \frac{1}{4} = \frac{1}{4}$.

d. Für jedes $E_K(\cdot)$ gibt der oben (zu Aufgabe 3.1 d) beschriebene Angreifer den Wert 1 aus, deshalb gilt $\Pr_{K\in_\$\mathcal{K}}\left[\boldsymbol{A}^{E_K(\cdot)} \Rightarrow 1\right] = 1$.

Für $f(\cdot)$ könnten wir wieder die verschiedenen Fälle tabellieren. Das sind 256 ($= 4^4$) verschiedene Abbildungen, deshalb fassen wir sie in Gruppen von jeweils 16 Abbildungen zusammen, indem wir nur nach den (für $\boldsymbol{A}$ allein relevanten) Werten zu den Argumenten 00 und 01 unterscheiden.

$f = \ldots$	$f(00)$	$f(01)$	$\ldots$	$\boldsymbol{A}^{f(\cdot)} \Rightarrow \ldots$
$f_1, \ldots, f_{16}$	00	00		0
$f_{17}, \ldots, f_{32}$	00	01		1
$f_{33}, \ldots, f_{48}$	00	10		0
$f_{49}, \ldots, f_{64}$	00	11		0
$f_{65}, \ldots, f_{80}$	01	00		0
$f_{81}, \ldots, f_{96}$	01	01		0
$f_{97}, \ldots, f_{112}$	01	10		1
$f_{113}, \ldots, f_{128}$	01	11		0
$f_{129}, \ldots, f_{144}$	10	00		0
$f_{145}, \ldots, f_{160}$	10	01		0
$f_{161}, \ldots, f_{176}$	10	10		0
$f_{177}, \ldots, f_{192}$	10	11		1
$f_{193}, \ldots, f_{208}$	11	00		1
$f_{209}, \ldots, f_{224}$	11	01		0
$f_{225}, \ldots, f_{240}$	11	10		0
$f_{241}, \ldots, f_{256}$	11	11		0

In vier von sechzehen Fällen aus dieser Tabelle gibt $\boldsymbol{A}$ hier das Ergebnis 1 aus, also bei $4 \cdot 16 = 64$ von $16 \cdot 16 = 256$ Abbildungen. Somit ergibt sich hier $\Pr_{f\in_\$\mathrm{Func}(\{0,1\}^2)}\left[\boldsymbol{A}^{f(\cdot)} \Rightarrow 1\right] = \frac{64}{256} = \frac{1}{4}$.

Es folgt $\mathrm{Adv}^{\mathsf{PRF}}_{E_K,\boldsymbol{A}} = \Pr_{K\in_\$\mathcal{K}}\left[\boldsymbol{A}^{E_K(\cdot)} \Rightarrow 1\right] - \Pr_{f\in_\$\mathrm{Func}(\{0,1\}^2)}\left[\boldsymbol{A}^{f(\cdot)} \Rightarrow 1\right] = \frac{3}{4}$.