Problem 1: Fun With One Way Functions

a. Here is how we can invert \( f_a \). On input \( y \), choose \( x'_1 \) at random. Let \( x'_2 = f(x'_1) \oplus y \), and let our proposed preimage for \( y \) be \( x' = x'_1 \odot x'_2 \).

\[
\begin{align*}
  f_a(x') &= f(x'_1) \oplus x'_2 \\
  &= f(x'_1) \oplus (f(x'_1) \oplus y) \\
  &= y
\end{align*}
\]

b. The error is that \( f(x'_1) \oplus x'_2 = y \oplus z \) does not imply that \( f(x'_1) = y \) and \( x'_2 = z \).

c. Proof. Let \( f \) be a one way function, and fix some polynomial \( p \). We claim that there exists some \( n_0 \) such that, \( \forall n > n_0 \),

\[
|\{ f(x) : x \in \{0, 1\}^n \}| > p(n).
\]

Assume, for the sake of contradiction, that the above is false: no such \( n_0 \) exists, and thus there exist arbitrarily large \( n \)'s such that the image of \( f \) has cardinality no larger than \( p(n) \). Recall the definition of a one-way function being ‘hard to invert’:

\[
\Pr_{x \leftarrow \{0, 1\}^n; \ x' \leftarrow A(1^n, f(x)) : f(x') = f(x)} = \nu(n)
\]

for all \( n \), for all PPT \( A \) and for some negligible \( \nu \).

Consider a PPT \( B \) which, on input \( f(x) = y \), uses its random tape to repeatedly sample some \( x' \) from \( \{0, 1\}^n \), and output it if \( f(x') = f(x) \) (looping until it finds such a \( x' \)). By assumption, there exist arbitrarily large \( n \) where the probability that \( f(x') = f(x) \) for a randomly chosen \( x' \) is at least \( \frac{1}{p(n)} \), since the average probability of getting any particular element in the range is necessarily the inverse of its cardinality.\(^1\) Thus, \( B \) has expected polynomial-runtime. Correctness follows from our condition that \( B \) loops until it finds a valid preimage of \( y \).

This means that there cannot exist a \( \nu \) such that

\[
\Pr_{x \leftarrow \{0, 1\}^n; \ x' \leftarrow A(1^n, f(x)) : f(x') = f(x)} = \nu(n)
\]

for all \( n \), because there exist arbitrarily large \( n \)'s for any \( p \) such that \( B \) can invert the function with probability better than \( \frac{1}{p(n)} \). This contradicts our assumption that \( f \) is a one-way function, and thus one-way functions must have larger-than-polynomial ranges for sufficiently large \( n \).

\( \square \)

d. Proof. Suppose there is some algorithm \( A \) which can invert \( g \) with non-negligible probability. We here show that we can use \( A \) to construct a new algorithm, \( B \), which inverts \( f \).

Define \( B \) to do the following on input \( y = f(x) \), where \( x \) has length \( k \):

\[
\sum_{y \leftarrow \text{Range}} \Pr_{\text{Pr}} = \frac{1}{|\text{Range}|}
\]
(a) Run $\mathcal{A}$ on $y$, which gives us some $x' = x'_1 \circ x'_2$
(b) Return $x'_1$

If $\mathcal{A}$ gave us an $x'$ such that $g(x') = y$, that means (by definition of $g$) that $f(x'_1) = y$, and thus $B$ will be correct whenever $\mathcal{A}$ was correct. Considering that our distribution of inputs to $\mathcal{A}$ is identical to what it would receive in the wild, $B$ will be correct with the same nonnegligible probability as $\mathcal{A}$.

This contradicts our assumption that $f$ is one-way, and thus $g$ must also be one-way.

\square

Problem 2: Definitions of Indistinguishability

a. First, we show that Definition 2 implies Definition 1. Assuming Definition 2 holds, we wish to show that for all $\mathcal{A}$, $c_\mathcal{A}(k)$ is upper bounded by one-half plus a negligible function.

(a) Let $\mathcal{A}$ be fixed. Define

$$c_{\mathcal{A},1}(k) = \Pr[x \leftarrow D_1(1^k); i' \leftarrow \mathcal{A}(1^k, x) : i' = 1].$$

In other words, $c_{\mathcal{A},1}(k)$ is the probability that $\mathcal{A}$ is correct given that $x$ comes from $D_1$. Similarly, define

$$c_{\mathcal{A},2}(k) = \Pr[x \leftarrow D_2(1^k); i' \leftarrow \mathcal{A}(1^k, x) : i' = 2].$$

We immediately derive

$$c_\mathcal{A}(k) = \frac{1}{2}c_{\mathcal{A},1} + \frac{1}{2}c_{\mathcal{A},2}.$$

(b) Define $\mathcal{A}'(1^k, x)$ as follows: Run $\mathcal{A}(1^k, x)$. Output 0 if $\mathcal{A}$ outputs 1, and output $-1$ otherwise.

$$z_{\mathcal{A}',1}(k) = c_{\mathcal{A},1}(k)$$
$$z_{\mathcal{A}',2}(k) = 1 - c_{\mathcal{A},2}(k)$$

(c)

$$c_{\mathcal{A},1}(k) = z_{\mathcal{A}',1}(k)$$
$$c_{\mathcal{A},2}(k) = 1 - z_{\mathcal{A}',2}(k)$$

(d) $c_\mathcal{A}(k) = \frac{1}{2}z_{\mathcal{A}',1}(k) + \frac{1}{2}(1 - z_{\mathcal{A}',2}(k))$

(e) If Definition 2 holds, then there exists a negligible $\nu$ such that $|z_{\mathcal{A}',1}(k) - z_{\mathcal{A}',2}(k)| \leq \nu(k)$. From there,

$$c_\mathcal{A}(k) = \frac{1}{2} + \frac{1}{2}(z_{\mathcal{A}',1}(k) - z_{\mathcal{A}',2}(k))$$
$$c_\mathcal{A}(k) \leq \frac{1}{2} + \frac{1}{2}|z_{\mathcal{A}',1}(k) - z_{\mathcal{A}',2}(k)|$$
$$c_\mathcal{A}(k) \leq \frac{1}{2} + \frac{1}{2}\nu(k)$$

Therefore $c_\mathcal{A}(k)$ is bounded by one-half plus a negligible function, which is what we wished to show.

b. (a) Fix $\mathcal{A}'$ and $k$. 

HW 3 – Solutions-2
Case 1: $z_{A',1}(k) \geq z_{A',2}(k)$
Define $A(1^k, x)$ as follows: Run $A'(1^k, x)$. If $A'$ outputs 0, output 1, otherwise output 2. Recall that
$$c_A(k) = \frac{1}{2}c_{A,1}(k) + \frac{1}{2}c_{A,2}(k).$$
When combined with our results from part a.(c), namely,
$$c_{A,1}(k) = z_{A',1}(k)$$
$$c_{A,2}(k) = 1 - z_{A',2}(k)$$
we find that
$$c_A(k) = \frac{1}{2}z_{A',1}(k) + \frac{1}{2}(1 - z_{A',2}(k))$$
Since $z_{A',1}(k) \geq z_{A',2}(k)$,
$$c_A(k) = \frac{1}{2} + \frac{1}{2}|z_{A',1}(k) - z_{A',2}(k)|.$$ 

Case 2: $z_{A',1}(k) < z_{A',2}(k)$
Define $A(1^k, x)$ as follows: Run $A'(1^k, x)$. If $A'$ outputs 0, output 2, otherwise output 1. Similar to case 1,
$$c_{A,1}(k) = 1 - z_{A',1}(k)$$
$$c_{A,2}(k) = z_{A',2}(k)$$
and thus
$$c_A(k) = \frac{1}{2}(1 - z_{A',1}(k)) + \frac{1}{2}z_{A',2}(k)$$
Since $z_{A',1}(k) < z_{A',2}(k)$,
$$c_A(k) = \frac{1}{2} + \frac{1}{2}|z_{A',1}(k) - z_{A',2}(k)|.$$ 

(b) A circuit is a different model of computation than Turing machines in which you can have an algorithm specific to each input size; thus, we may define each $A_k$ or $A'_k$ to be dependent on the security parameter $k$. For each $A' = \{A'_k\}$, we can define $A = \{A_k\}$ by defining each $A_k$ in terms of each $A'_k$ as above. Then for each $k$ we have
$$c_A(k) = \frac{1}{2} + \frac{1}{2}|z_{A',1}(k) - z_{A',2}(k)|$$
If Definition 1 holds, then there exists a negligible function $\nu$ such that $c_A(k) \leq \frac{1}{2} + \nu(k)$ for $k$ large enough. Then for $k$ large enough, we have that
$$\nu(k) \geq \frac{1}{2}|z_{A',1}(k) - z_{A',2}(k)|,$$
so $|z_{A',1}(k) - z_{A',2}(k)|$ is negligible.

**Problem 3: Statistical Indistinguishability**

a. If $\Pr[x \leftarrow D_{0,k} : x = \hat{x}] > \Pr[x \leftarrow D_{1,k} : x = \hat{x}]$, then Dave should pick 0 since it is more likely that $\hat{x}$ is in $S_{0,k}$. Otherwise, Dave should pick 1.
b. First we note that if the only possible outputs of Test are 0 and 1 then it must be the case that

\[ \Pr[x \leftarrow D_{1,k} : b' \leftarrow \text{Test}(x) : b' = 0] + \Pr[x \leftarrow D_{1,k} : b' \leftarrow \text{Test}(x) : b' = 1] = 1, \]

which we can also write as

\[ p_1(\text{Test}) + \Pr[x \leftarrow D_{1,k} : b' \leftarrow \text{Test}(x) : b' = 1] = 1. \]

To show that \( \text{Adv}(\text{Test}) = \text{Adv}'(\text{Test}) \), we see that

\[
\text{Adv}(\text{Test}) = \left| \Pr[b \leftarrow \{0,1\} ; x \leftarrow D_{b,k} : b' \leftarrow \text{Test}(x) : b' = b] - 1/2 \right| = \left| \Pr[b \leftarrow \{0,1\} ; x \leftarrow D_{b,k} : b' \leftarrow \text{Test}(x) : b' = 0] - \Pr[b \leftarrow \{0,1\} ; x \leftarrow D_{b,k} : b' \leftarrow \text{Test}(x) : b' = 1] \right| - 1/2
\]

(1)

\[
= \left| \Pr[b \leftarrow \{0,1\} ; x \leftarrow D_{b,k} : b' \leftarrow \text{Test}(x) : b' = b] - 1/2 \right| \cdot \Pr[b = 0]
\]

(2)

\[
+ \Pr[b \leftarrow \{0,1\} ; x \leftarrow D_{b,k} : b' \leftarrow \text{Test}(x) : b' = 0] \cdot \Pr[b = 0]
\]

(3)

\[
= \left| \Pr[x \leftarrow D_{0,k} : b' \leftarrow \text{Test}(x) : b' = 0] \right| \cdot \Pr[b = 0]
\]

(4)

\[
+ \Pr[x \leftarrow D_{0,k} : b' \leftarrow \text{Test}(x) : b' = 1] \cdot \Pr[b = 1] - 1/2
\]

(5)

\[
= \left| \Pr[x \leftarrow D_{0,k} : b' \leftarrow \text{Test}(x) : b' = 0] - \Pr[x \leftarrow D_{0,k} : b' \leftarrow \text{Test}(x) : b' = 1] \right|/2
\]

(6)

\[
= \left| \Pr[\text{po}(\text{Test}) - p_1(\text{Test})] \right|/2
\]

(7)

\[
= \text{Adv}'(\text{Test})
\]

(8)

where Equation (6) follows from Equation (5) by the fact that we know the distributions are equally likely, and Equation (7) follows from Equation (6) by the symmetry of absolute value and the discussion above.

c. To do this, we wish to show that there is some kind of relationship between the statistical difference and the advantage of the optimal algorithm:

\[
\Delta(D_{0,k}, D_{1,k}) = \frac{1}{2} \sum_{x} \left| \Pr[x \leftarrow D_{1,k} : x = \hat{x}] - \Pr[x \leftarrow D_{0,k} : x = \hat{x}] \right|
\]

\[
= \frac{1}{2} \sum_{\hat{x}} \left| P_{1,k}(\hat{x}) - P_{0,k}(\hat{x}) \right|
\]

\[
= \frac{1}{2} \left( \sum_{\hat{x} \mid P_{0,k}(\hat{x}) < P_{1,k}(\hat{x})} \left| P_{1,k}(\hat{x}) - P_{0,k}(\hat{x}) \right| + \sum_{\hat{x} \mid P_{0,k}(\hat{x}) \geq P_{1,k}(\hat{x})} \left| P_{0,k}(\hat{x}) - P_{1,k}(\hat{x}) \right| \right)
\]

\[
= \frac{1}{2} \left( \sum_{\hat{x} \mid P_{0,k}(\hat{x}) < P_{1,k}(\hat{x})} P_{1,k}(\hat{x}) - P_{0,k}(\hat{x}) + \sum_{\hat{x} \mid P_{0,k}(\hat{x}) \geq P_{1,k}(\hat{x})} P_{0,k}(\hat{x}) - P_{1,k}(\hat{x}) \right)
\]

(9)

Note that we can drop the absolute values in the third line because we have separated the sum into portions. We can then add back in the absolute values on the fourth line because both quantities are positive, and adding an absolute value doesn’t affect it.

For all of the \( \hat{x} \) with the property that \( P_{0,k}(\hat{x}) \geq P_{1,k}(\hat{x}) \), we know that \( \Pr[b \leftarrow \text{Test}(\hat{x}) : b = 0] = 1 \), because the optimal Test algorithm will always return 1 if the probability of \( x \) in distribution 0 is higher than its probability in distribution 1. This means that:

\[
\sum_{\hat{x} \mid P_{0,k}(\hat{x}) \geq P_{1,k}(\hat{x})} P_{0,k}(\hat{x}) = \sum_{\hat{x} \mid P_{0,k}(\hat{x}) \geq P_{1,k}(\hat{x})} \Pr[b \leftarrow \text{Test}(\hat{x}) : b = 0] \cdot \Pr[x \leftarrow D_{0,k} : x = \hat{x}]
\]
For all other values of \( \hat{x} \), we know that \( \Pr[b \leftarrow \text{Test}(\hat{x}) : b = 0] = 0 \). Therefore:

\[
\sum_{\hat{x} \mid P_0, k(\hat{x}) < P_1, k(\hat{x})} \Pr[b \leftarrow \text{Test}(\hat{x}) : b = 0] \cdot \Pr[x \leftarrow D_{0, k} : x = \hat{x}] = 0
\]

We can then combine that equation with the one before it, adding zeroes to both sides, to get:

\[
\sum_{\hat{x} \mid P_0, k(\hat{x}) \geq P_1, k(\hat{x})} P_0, k(\hat{x}) = \sum_{\hat{x} \mid P_0, k(\hat{x}) \geq P_1, k(\hat{x})} \Pr[b \leftarrow \text{Test}(\hat{x}) : b = 0] \cdot \Pr[x \leftarrow D_{0, k} : b = \text{Test}(x) : b = 0]
= p_0(\text{Test})
\]

We can perform similar transformations to find that:

\[
\sum_{\hat{x} \mid P_0, k(\hat{x}) \geq P_1, k(\hat{x})} P_1, k(\hat{x}) = \Pr[x \leftarrow D_{1, k} : b = \text{Test}(x) : b = 0] = p_1(\text{Test})
\]

\[
\sum_{\hat{x} \mid P_0, k(\hat{x}) < P_1, k(\hat{x})} P_0, k(\hat{x}) = 1 - p_0(\text{Test})
\]

\[
\sum_{\hat{x} \mid P_0, k(\hat{x}) < P_1, k(\hat{x})} P_1, k(\hat{x}) = 1 - p_1(\text{Test})
\]

We can then substitute those values into our first equation to get:

\[
\Delta(D_{0, k}, D_{1, k}) = \frac{1}{2} \left( \left| \sum_{\hat{x} \mid P_0, k(\hat{x}) < P_1, k(\hat{x})} P_{1, k}(\hat{x}) - P_{0, k}(\hat{x}) \right| + \left| \sum_{\hat{x} \mid P_0, k(\hat{x}) \geq P_1, k(\hat{x})} P_{0, k}(\hat{x}) - P_{1, k}(\hat{x}) \right| \right)
= \frac{1}{2} \left( \left| (1 - p_1(\text{Test})) - (1 - p_0(\text{Test})) \right| + \left| |p_0(\text{Test}) - p_1(\text{Test})| \right| \right)
= |p_0(\text{Test}) - p_1(\text{Test})| = 2\text{Adv}^\prime(\text{Test})
\]

Because they only differ by a factor of two, if one of the two is negligible, then so is the other. This means that two distributions are statistically indistinguishable if and only if their statistical distance is negligible.

HW 3 – Solutions-5