CS6111: Foundations of Cryptography

Assignment 3 - CS16B107

Instructions

- Deadline: Wednesday, Oct 16.
- We encourage submissions by Latex. Paper is also accepted.

References

- Introduction to Cryptography - Delfs and Knebl
- A Graduate Course in Applied Cryptography - Boneh and Shoup (link)
- Introduction to Modern Cryptography - Katz and Lindell

1 Number Theory

Let G be some group and let $g \in G$ be an element of prime order n. That is, the set of elements generated by g is a cyclic group of prime order, denoted as follows: $G_n = \langle g \rangle = \{g^i \mid i \geq 0\}$. We have that $\langle g \rangle^* = \{g^x : x \in \mathbb{Z}_n^*\}$ is the set of all generators of G_n. Clearly, $|\langle g \rangle^*| = \phi(n)$, which is known to be the number of generators of any cyclic group of order n.

1. (8 points) Show that for any $h \in \langle g \rangle$, the following conditions are equivalent:

   (1) $h \in \langle g \rangle^*$

   (2) $ord(h) = n$

   (3) $\langle h \rangle = \langle g \rangle$

   (4) $\langle h \rangle^* = \langle g \rangle^*$

   To show equivalency, you must prove the following:

   (a) (2 points) (1) $\implies$ (2)

   (b) (2 points) (2) $\implies$ (3)

   (c) (2 points) (3) $\implies$ (4)

   (d) (2 points) (4) $\implies$ (1)

Solution:

(a) h is a generator of $\langle g \rangle$.

$\implies h^n = i$ and n is the smallest integer that satisfies this. By definition, the order of h is the smallest positive integer i with $h^i = 1$.

$\implies ord(h) = n$

(b)

$$ord(h) = n$$

$$\implies |\langle h \rangle| = |\{h^i \mid i \geq 0\}| = n$$

Since $|\langle h \rangle| = |G_n|$ and $\langle h \rangle \subseteq G_n$, we have

$$\langle h \rangle = G_n = \langle g \rangle$$

(c) $langleh\rangle = \langle g \rangle$. Thus the set of generators of these two sets are the same as well. Thus $\langle h \rangle^* = \langle g \rangle^*$.

(d) Since h is a generator of $\langle h \rangle$ (by construction), we have $h \in \langle h \rangle^*$. Thus, given $\langle h \rangle^* = \langle g \rangle^*$, we have $h \in \langle g \rangle^*$.

2. (2 points) Show that $a^{\log_h b} = b^{\log_h a}$ for any $a, b \in \langle g \rangle$ and $h \in \langle g \rangle^*$.

Solution: h is a generator of $\langle g \rangle$. Let i, j be the smallest positive integers such that $h^i = a$ and $h^j = b$.

$$a^{\log_h b} = a^j = (h^i)^j = h^{ij}$$

$$b^{\log_h a} = b^i = (h^j)^i = h^{ij} = a^{\log_h b}$$

2 Probability Theory

Let X, Y be two random variables and V denote the set of possible values for X and Y. $\Delta(X;Y)$ represents the statistical distance between X and Y.

1. (2 points) Prove the following proposition: $\Delta(X;Y) = 1 - \sum_{v \in V} \min(\Pr[X = v], \Pr[Y = v])$.

Solution: Let $V_x = \{u \mid u \in V \; and \; X(u) \leq Y(u)\}$ and $V_y = V - V_x$.

$$\begin{aligned} 1 - \sum_{v \in V} \min(\Pr[X = v], \Pr[Y = v]) &= 1 - \sum_{v \in V_x} \min(\Pr[X = v], \Pr[Y = v]) - \sum_{v \in V_y} \min(\Pr[X = v], \Pr[Y = v]) \\ &= (1 - \sum_{v \in V_x} \Pr[X = v]) - \sum_{v \in V_y} \Pr[Y = v] \\ &= \sum_{v \in V_y} \Pr[X = v] - \sum_{v \in V_y} \Pr[Y = v] \end{aligned}$$

$$\implies LHS = \sum_{v \in V_y} |\Pr[X = v] - \Pr[Y = v]|$$

Similarly,

$$\begin{aligned} LHS &= (1 - \sum_{v \in V_y} \Pr[Y = v]) - \sum_{v \in V_x} \Pr[X = v] \\ &= \sum_{v \in V_x} \Pr[Y = v] - \sum_{v \in V_x} \Pr[X = v] \\ &= \sum_{v \in V_x} |\Pr[X = v] - \Pr[Y = v]| \end{aligned}$$

Adding the above two statements and dividing by two,

$$\begin{aligned} LHS &= \frac{1}{2}(\sum_{v \in V_x} |\Pr[X = v] - \Pr[Y = v]| + \sum_{v \in V_y} |\Pr[X = v] - \Pr[Y = v]|) \\ &= \frac{1}{2} \sum_{v \in V} |\Pr[X = v] - \Pr[Y = v]| \\ &= \Delta(X; Y) \end{aligned}$$

2. (2 points) Prove the triangle inequality: $\Delta(X; Z) \leq \Delta(X; Y) + \Delta(Y; Z)$

Solution: Notation: $X(u) = Pr[X = u]$.

$$\forall u \in V \;\; |X(u) - Z(u)| = |(X(u) - Y(u)) + (Y(u) - Z(u))| \leq |X(u) - Y(u)| + |Y(u) - Z(u)|$$

Summing over all u and dividing by 2,

$$\frac{1}{2} \sum_{\{} u \in V\} |X(u) - Z(u)| \leq \frac{1}{2} \sum_{\{} u \in V\} |X(u) - Y(u)| + \frac{1}{2} \sum_{\{} u \in V\} |Y(u) - Z(u)|$$

$$\implies \Delta(X; Z) \leq \Delta(X; Y) + \Delta(Y; Z)$$

3. (2 points) Prove that $\Delta(f(X); f(Y)) \leq \Delta(X; Y)$ for any function f defined on V.

Solution: Let W be the range of f. Let X_f and Y_f be the distributions on the range obtained when f is applied on the domain V with distributions X and Y respectively.

$$\begin{aligned} \Delta(f(X); f(Y)) &= \frac{1}{2}(\sum_{v \in W} |X_f[v] - Y_f[v]|) \\ &= \frac{1}{2} \left(\sum_{v \in W} \left| \sum_{u: f(u) = v} X[u] - \sum_{u: f(u) = v} Y[u] \right| \right) \end{aligned}$$

$$\implies \Delta(f(X); f(Y)) = \frac{1}{2}\left(\sum_{v\in W}\left|\sum_{u:f(u)=v}(X[u]-Y[u])\right|\right)$$
$$\leq \frac{1}{2}\left(\sum_{v\in W}\sum_{u:f(u)=v}|X[u]-Y[u]|\right)$$
$$= \frac{1}{2}\left(\sum_{v\in W}\sum_{u:f(u)=v}|X[u]-Y[u]|\right)$$

Thus, since each $u \in V$ has at most one image in W, we have

$$\implies \Delta(f(X); f(Y)) \leq \frac{1}{2}\left(\sum_{u\in V}|X[u]-Y[u]|\right) = \Delta(X;Y)$$

4. (4 points) For $n \geq 1$, let $X \in_R \mathbb{Z}_n$ and $Y \in_R \mathbb{Z}_n^*$.
   (a) (2 points) Determine $\Delta(X;Y)$.
   (b) (2 points) Show that $\Delta(X+Y; XY) = 0$, where addition and multiplication are done modulo n.

Solution:

(a)

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$$
$$\mathbb{Z}_n^* = \{a \in \{1, \ldots, n-1\} | gcd(a,n) = 1\} \implies |\mathbb{Z}_n^*| = \phi(n)$$

Thus, the distributions are given by

$$X(a) = \begin{cases} \frac{1}{n} & \text{for } a \in \mathbb{Z}_n \\ 0 & \text{otherwise} \end{cases}$$

$$Y(a) = \begin{cases} \frac{1}{\phi(n)} & \text{for } a \in \mathbb{Z}_n^* \\ 0 & \text{otherwise} \end{cases}$$

We know that $\mathbb{Z}_n^* \subseteq \mathbb{Z}_n$. Let $B = \mathbb{Z}_n - \mathbb{Z}_n^*$. Also, $n \geq \phi(n)$.

$$\implies \Delta(X;Y) = \frac{1}{2}(\sum_{a\in\mathbb{Z}_n}|X[a]-Y[a]|)$$
$$= \frac{1}{2}((\sum_{a\in\mathbb{Z}_n^*}|X[a]-Y[a]|) + (\sum_{a\in B}|X[a]-Y[a]|))$$
$$= \frac{1}{2}\left(\sum_{a\in\mathbb{Z}_n^*}(\frac{1}{\phi(n)}-\frac{1}{n}) + \sum_{a\in B}(\frac{1}{n}-0)\right)$$
$$= \frac{1}{2}\left(\phi(n)(\frac{1}{\phi(n)}-\frac{1}{n}) + (n-\phi(n))(\frac{1}{n})\right)$$

$$\Delta(X;Y) = 1 - \frac{\phi(n)}{n}$$

(b) Since X and Y are uniform distributions, we can directly compute distributions X+Y and XY by counting the number of occurrences.

Total no. of combinations for X and Y = $|\mathbb{Z}_n| * |\mathbb{Z}_n^*| = n\phi(n)$.
Let $a, c \in \mathbb{Z}_n$ and $b \in \mathbb{Z}_n^*$. For any given choice of c, we have

(a) X+Y

$$(a+b) mod n = c$$

For any option of $b \in \mathbb{Z}_n*$, there is exactly one choice of $a \in \mathbb{Z}_n$ (the unique inverse) that satisfies the above equation. Thus, no. of combinations for X and Y such that X+Y=c is $|\mathbb{Z}_n^*| = \phi(n)$.

$$Pr[X+Y=c] = \frac{\phi(n)}{n\phi(n)} = \frac{1}{n}$$

(b) XY

$$(ab) mod n = c$$

For any option of $b \in \mathbb{Z}_n*$, there is exactly one choice of $a \in \mathbb{Z}_n$ (the unique inverse which exists in $\mathbb{Z}_n^*$ since b is invertible by definition) that satisfies the above equation. Thus, no. of combinations for X and Y such that XY=c is $|\mathbb{Z}_n^*| = \phi(n)$.

$$Pr[XY=c] = \frac{\phi(n)}{n\phi(n)} = \frac{1}{n}$$

Since $Pr[X+Y=c] = Pr[XY=c]\ \forall\ c$, the two distributions are the same. Hence $\Delta(X+Y;XY) = 0$.

5. (2 points) For $n \geq d \geq 1$, let random variable X take on values in $\{0, \cdots, d-1\}$, and let $U \in_R \{0, \cdots, n-1\}$. Show that $\Delta(U; X+U) \leq (d-1)/n$, and that this bound is tight.

Solution: Notation: $(X+U)(y) = Pr[X+U=y]$. Consider any c in the range of values $\{0, \ldots, n+d-2\}$. We need $a+b=y$, where a and b come from distributions X and U respectively. For any $a \in \{0, \ldots, d-1\}$, there exists at most one value of $b \in \{0, \ldots, n-1\}$ that satisfies the required equation. Thus, if we assume there is always a b that satisfies the condition, we get an upperbound on $(X+U)(y)$ as

$$(X+U)(y) \leq \sum_{a \in \{0,\ldots,d-1\}} X(a)U(y-a) = \sum_{a \in \{0,\ldots,d-1\}} X(a)\frac{1}{n} = \frac{1}{n} \sum_{a \in \{0,\ldots,d-1\}} X(a)$$

$$(X+U)(y) \leq \frac{1}{n}\ ,\ \forall y \tag{1}$$

Further, the above assumption of existence of $b \in \{0, \ldots, n-1\}$ for any $a \in \{0, \ldots, d-1\}$ is true for all $y \in \{d-1, \ldots, n-1\}$. Let $P = \{0, \ldots, d-2\}$, $Q = \{d-1, \ldots, n-1\}$, $R = \{n, \ldots, n+d-2\}$. (Note that sets P and R could be empty)

$$(X+U)(y) = \frac{1}{n}\ ,\ \forall y \in Q \tag{2}$$

$$\begin{aligned}
\Delta(U; X+U) &= \frac{1}{2}\sum_y |U(y) - (X+U)(y)| \\
&= \frac{1}{2}\left(\sum_{y\in P}|U(y)-(X+U)(y)| + \sum_{y\in Q}|U(y)-(X+U)(y)| + \sum_{y\in R}|U(y)-(X+U)(y)|\right) \\
&= \frac{1}{2}\left(\sum_{y\in P}|\frac{1}{n}-(X+U)(y)| + \sum_{y\in Q}|\frac{1}{n}-\frac{1}{n}| + \sum_{y\in R}|0-(X+U)(y)|\right) \quad (from\ (2)) \\
&\leq \frac{1}{2}\left(\sum_{y\in P}\frac{1}{n} + \sum_{y\in Q}0 + \sum_{y\in R}\frac{1}{n}\right) \quad (from\ (1)) \\
&= \frac{1}{2}\left(\frac{(d-2)-0+1}{n} + 0 + \frac{(n+d-2)-(n-1)+1}{n}\right) \\
&= \frac{d-1}{n}
\end{aligned}$$

We see that the equality is attained when the distribution of X given by

$$X(a) = \begin{cases} 1 & \text{if a = d-1} \\ 0 & \text{otherwise} \end{cases}$$

Hence it is a tight upperbound.

6. (4 points) For $n \geq 1$, consider distributions X, Y, Z given by

$$X = \{u : u \in_R \{0, \cdots, n-1\}\},$$
$$Y = \{2u : u \in_R \{0, \cdots, n-1\}\},$$
$$Z = \{2u+1 : u \in_R \{0, \cdots, n-1\}\}.$$

Clearly, $\Delta(Y; Z) = 1$.

(a) (2 points) Show that $\Delta(X; Y) = \Delta(X; Z) = 1/2$ for even n

(b) (2 points) Determine $\Delta(X; Y)$ and $\Delta(X; Z)$ for odd n.

Solution: Let $P = X \cap Y$ and $Q = X \cap Z$. The distributions X, Y and Z are all uniform distributions over sets of size n and hence assign probability $\frac{1}{n}$ to each of their elements.

(a) n is even. $|P| = n/2$. $|Q| = n/2$.

$$\begin{aligned}
\Delta(X; Y) &= \frac{1}{2}\left(\sum_{a\in X-P}|\frac{1}{n}-0| + \sum_{a\in P}|\frac{1}{n}-\frac{1}{n}| + \sum_{a\in Y-P}|0-\frac{1}{n}|\right) \\
&= \frac{1}{2}\left(\frac{n}{2}.\frac{1}{n} + \frac{n}{2}.0 + \frac{n}{2}.\frac{1}{n}\right) = \frac{1}{2}
\end{aligned}$$

$$\Delta(X; Z) = \frac{1}{2}\left(\sum_{a\in X-Q}|\frac{1}{n}-0| + \sum_{a\in Q}|\frac{1}{n}-\frac{1}{n}| + \sum_{a\in Z-Q}|0-\frac{1}{n}|\right)$$

$$\implies \Delta(X;Z) = \frac{1}{2}\left(\frac{n}{2}.\frac{1}{n} + \frac{n}{2}.0 + \frac{n}{2}.\frac{1}{n}\right) = \frac{1}{2}$$

(b) n is odd. $|P| = (n+1)/2$. $|Q| = (n-1)/2$.

$$\begin{aligned}\Delta(X;Y) &= \frac{1}{2}\left(\sum_{a\in X-P}|\frac{1}{n}-0| + \sum_{a\in P}|\frac{1}{n}-\frac{1}{n}| + \sum_{a\in Y-P}|0-\frac{1}{n}|\right)\\ &= \frac{1}{2}\left((n-\frac{n+1}{2}).\frac{1}{n} + \frac{n+1}{2}.0 + (n-\frac{n+1}{2}).\frac{1}{n}\right)\\ &= \frac{n-1}{2n}\end{aligned}$$

$$\begin{aligned}\Delta(X;Z) &= \frac{1}{2}\left(\sum_{a\in X-Q}|\frac{1}{n}-0| + \sum_{a\in Q}|\frac{1}{n}-\frac{1}{n}| + \sum_{a\in Z-Q}|0-\frac{1}{n}|\right)\\ &= \frac{1}{2}\left((n-\frac{n-1}{2}).\frac{1}{n} + \frac{n-1}{2}.0 + (n-\frac{n-1}{2}).\frac{1}{n}\right)\\ &= \frac{n+1}{2n}\end{aligned}$$

7. (5 points) For n prime, let h and M_0 be arbitrary, fixed elements of $G_n = \langle g\rangle, h \neq 1$. Consider distributions X, Y, Z given by

$$\begin{aligned}X &= \{(A,B) : A \in_R \langle g\rangle, B \in_R \langle g\rangle\},\\ Y &= \{(g^u, h^u M) : u \in_R \mathbb{Z}_n, M \in_R \langle g\rangle\},\\ Z &= \{(g^u, h^u M_0) : u \in_R \mathbb{Z}_n\}.\end{aligned}$$

(a) (2 points) Show that $\Delta(X;Y) = 0$

(b) (2 points) Show that $\Delta(Y;Z) = 1 - 1/n$

(c) (1 point) Show that $\Delta(X;Z) = 1 - 1/n$?

Solution:

Observation 1:

Since g is a generator, there exists a fixed $d \in \mathbb{Z}_n$ such that $g^d = h$.

Observation 2:

$\langle g\rangle$ is a cyclic group of prime order with g as a generator. Thus we have a mapping $f : \mathbb{Z}_n \to \langle g\rangle$ given by $f(a) = g^a$ as an isomorphism between $\mathbb{Z}_n$ and $\langle g\rangle$. Given this, choosing an $A \in_R \langle g\rangle$ is the same as producing g^u by choosing an $u \in_R \mathbb{Z}_n$, and vice versa.

(a) From observation 2, distribution X is the same as

$$X = \{(g^u, g^v) : u \in_R \mathbb{Z}_n, v \in_R \mathbb{Z}_n\}$$

From observations 1 and 2, distribution Y is same as

$$\begin{aligned} Y &= \{\left(g^u\ ,\ (g^d)^u(g^w)\right) : u \in_R \mathbb{Z}_n, w \in_R \mathbb{Z}_n\} \\ &= \{\left(g^u\ ,\ g^{(du+w) \mod n}\right) : u \in_R \mathbb{Z}_n, w \in_R \mathbb{Z}_n\} \end{aligned}$$

Since choosing $u \in_R \mathbb{Z}_n$ and $w \in_R \mathbb{Z}_n$ and producing $(du + w) \mod n \in_R \mathbb{Z}_n$ is same as choosing $v \in_R \mathbb{Z}_n$ (note that the distribution of $(du + w) \mod n$ is independent of u), we have

$$Y = \{(g^u, g^v) : u \in_R \mathbb{Z}_n, v \in_R \mathbb{Z}_n\} = X$$

Thus, $\Delta(X;Y) = 0$

(b) Similar to observation 1, let $g^k = M_0$. Thus, similar to previous part, we have

$$Z = \{\left(g^u\ ,\ g^{(du+k) \mod n}\right) : u \in_R \mathbb{Z}_n\}$$

Now, for computing statistical difference between the distributions, the value remains the same even if work on the other side of the isomorphism. Thus, let us have

$$Y = X = \{(u, v) : u \in_R \mathbb{Z}_n, v \in_R \mathbb{Z}_n\}$$

$$Z = \{(u, (du + k) mod\ n) : u \in_R \mathbb{Z}_n\}$$

Note that $Z \subseteq Y$. (overloading notation for Y and Z for the corresponding sets).

$$\begin{aligned} \Delta(Y;Z) &= \frac{1}{2} \sum_{(u,v)\in Y} |Y(u,v) - Z(u,v)| \\ &= \frac{1}{2} \left(\sum_{(u,v)\in Y-Z} |Y(u,v) - Z(u,v)| + \sum_{(u,v)\in Z} |Y(u,v) - Z(u,v)| \right) \\ &= \frac{1}{2} \left(\sum_{(u,v)\in Y-Z} |\frac{1}{n^2} - 0| + \sum_{(u,v)\in Z} |\frac{1}{n^2} - \frac{1}{n}| \right) \\ &= \frac{1}{2} \left((n^2 - n)\frac{1}{n^2} + n(\frac{1}{n} - \frac{1}{n^2}) \right) \\ &= 1 - \frac{1}{n} \end{aligned}$$

(c) Since $\Delta(X;Y) = 0$, it implies distributions X and Y are the same. Thus, $\Delta(X;Z) = \Delta(Y;Z) = 0$.

Omitted

8. (0 points) Prove the following proposition:

   1. $0 \le \Delta(X;Y) \le 1$, "nonnegativity" and "boundedness".
   2. $\Delta(X;Y) = 0$ if and only if $\forall_{v\in V} \Pr[X = v] = Pr[Y = v]$, "identical distributions".

3. $\Delta(X;Y) = \Delta(Y;X)$, "symmetry".
4. $\Delta(X;Z) \leq \Delta(X;Y) + \Delta(Y;Z)$. "triangle inequality".

9. (0 points) Prove the following proposition:
   1. $\Delta(X;Y) = \sum_{v \in V^+}(\Pr[X=v] - \Pr[Y=v])$, with $V^+ = \{v \in V : \Pr[X=v] > \Pr[Y=v]\}$.
   2. $\Delta(X;Y) = \sum_{v \in V}(\Pr[X=v] \dot{-} \Pr[Y=v])$, with $x \dot{-} y = \max(x-y, 0)$ ("x monus y").
   3. $\Delta(X;Y) = 1 - \sum_{v \in V} \min(\Pr[X=v], \Pr[Y=v])$.
   4. $\Delta(X;Y) = \max_{W \subseteq V} |\Pr[X \in W] - \Pr[Y \in W]|$.

10. (0 points) For $n, d \geq 1$, consider distributions X and Y given by

$$X = \{u : u \in_R \{0, \cdots, n-1\}\},$$
$$Y = \{u + d : u \in_R \{0, \cdots, n-1\}\}.$$

Determine $\Delta(X;Y)$, assuming $d \leq n$. Also, what is $\Delta(X;Y)$ if $d > n$?

3 One Way Functions/ Permutations

1. (2 points) Let $g_1 : \{0,1\}^n \to \{0,1\}^n$ and $g_2 : \{0,1\}^n \to \{0,1\}^n$ be two length preserving one-way functions. Define $f(x) = g_1(x)||g_2(x)$. Show that f is not necessarily a one way function.

Solution: Let us consider n to be even. (The case where n is odd can be handled similarly using $\lceil n/2 \rceil$ and $\lfloor n/2 \rfloor$) Let $h : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ be an one-way function. We define the two functions g_1 and g_2 on input $x = x_1||x_2$ (where $|x_1| = |x_2| = n/2$) as

$$g_1(x) = g_1(x_1||x_2) = x_1||h(x_2)$$

$$g_2(x) = g_2(x_1||x_2) = x_2||h(x_1)$$

Proof that g_2 is one-way: Let A be an attacker against the one-wayness of g_2, then we construct an attacker B against the one-wayness of h as follows: Upon input of y, B invokes A on input $0^{n/2}||y$. Eventually, A outputs $x_1'||x_2'$ and B outputs x_2'.
If A runs in polynomial time (in input length n) then B also runs in polynomial time (in input length n/2). Further, we also see that success probability of B is at least as good as that of A.

$$Pr[B(y) \in h^{-1}(y)] \geq Pr[A(0^{n/2}||y) \in g_2^{-1}(0^{n/2}||y)]$$

Therefore it follows that g_2 is one-way whenever h is. Similarly, we can show that g_1 is also one-way.

Now, let

$$f(x) = g_1(x)||g_2(x)$$

$$\implies f(x_1||x_2) = g_1(x_1||x_2)||g_2(x_1||x_2) = x_1||h(x_2)||x_2||(x_1)$$

Clearly $f(x) = f(x_1||x_2)$ is not one-way as the output contains both halves x_1 and x_2 of x.

2. (4 points) Let f_1 and f_2 be one way functions, where $\exists\ |x_1| = |x_2| \implies |f(x_1)| = |f(x_2)|$ (same sized output for same sized inputs). Let $f(x) = f_1(x_1) \oplus f_2(x_2)$ where $x = x_1||x_2$ and $|x_1| = |x_2|$ (assume even inputs).

   (a) Give an example where f_1, f_2 and f are one way functions.

   (b) Give an example where f_1, f_2 are one way but not f.

Solution:

(a) Let g be a one-way function that gives same sized outputs for same sized inputs. We define f_1 and f_2 as

$$f_1(x) = 0^{|g(x)|}||g(x)$$
$$f_2(x) = g(x)||0^{|g(x)|}$$

Clearly f_1 and f_2 produce same sized outputs for same sized inputs.

Proof that f_1 is one-way: Let A be an attacker against the one-wayness of f_1, then we construct an attacker B against the one-wayness of g as follows: Upon input of y, B invokes A on input $0^{|y|}||y$. Eventually, A outputs x' and B outputs x'.

If A runs in polynomial time (in input length n) then B also runs in polynomial time (in input length n). Further, we also see that success probability of B is at least as good as that of A.

$$Pr[B(y) \in g^{-1}(y)] \geq Pr[A(0^{|y|}||y) \in f_1^{-1}(0^{|y|}||y)]$$

Therefore it follows that f_1 is one-way whenever g is. Similarly, we can show that f_2 is also one-way.

$$f(x) = f(x_1||x_2) = f_1(x_1) \oplus f_2(x_2) = (0^{|g(x_1)|}||g(x_1)) \oplus (g(x_2)||0^{|g(x_2)|}) = g(x_2)||g(x_1)$$

Proof that f is one-way: Let A be an attacker against the one-wayness of f, then we construct an attacker B against the one-wayness of g as follows: Upon input of y, B invokes A on input $y||y$. Eventually, A outputs x'_1, x'_2 and B outputs x'_1.

If A runs in polynomial time (in input length n) then B also runs in polynomial time (in input length n/2). Further, we also see that success probability of B is at least as good as that of A. Thus f is a one-way function.

(b) Let g be a length preserving one-way function. We construct two new length preserving functions f_1, f_2 on even sized inputs (f_1 and f_2 can be proven to be one-way similar to the proof in question 1 of this section).

$$f_1(z) = f_1(z_1||z_2) = g(z_1)||z_2$$
$$f_2(z) = f_2(z_3||z_4) = z_3||g(z_4)$$

Now, for input x whose size is a multiple of 4, we have f as

$$\begin{aligned} f(x) &= f(x_1||x_2) \\ &= f_1(x_1) \oplus f_2(x_2) \\ &= f_1(z_1||z_2) \oplus f_2(z_3||z_4) \end{aligned}$$

$$f(x) = (g(z_1)||z_2) \oplus (z_3||g(z_4))$$
$$= (g(z_1) \oplus z_3)||(z_2 \oplus g(z_4))$$

Now, let $y = y_1||y_2$ (where $|y| = 2k$) be a given output of f that needs to be inverted by the adversary. Consider

$$x'_1 = z'_1||z'_2 = 0^k||(g(0^k) \oplus y_2)$$
$$x'_2 = z'_3||z'_4 = (g(0^k) \oplus y_1)||0^k$$

$$\implies g(z'_1) \oplus z'_3 = g(0^k) \oplus (g(0^k) \oplus y_1) = y_1$$
$$\implies z'_2 \oplus g(z'_4) = (g(0^k) \oplus y_2) \oplus g(0^k) = y_2$$
$$\implies f(x'_1||x'_2) = y_1||y_2$$

Thus, we can always invert f deterministically in polynomial time. Hence f is not one-way.

3. (8 points) Let $g(x)$ be a length preserving one-way function. Let $x = x_1||x_2$ where $x_1 = x_2$ (assume even inputs). Which of following are one-way functions? Prove your answers.

   (a) $f_a(x) = g(\bar{x})$, where $\bar{x}$ is the bitwise compliment of x

   (b) $f_b(x) = g(x_1 \oplus x_2)$

   (c) $f_c(x) = \begin{cases} 0^{|x|} \text{ if exactly one bit of } x_1 \text{ is 1} \\ 0^{|x_1|} \cdot g(x_2) \quad \text{otherwise} \end{cases}$

   (d) $f_d(x) = \begin{cases} 0^{|x|} \text{ if at least one bit of } x_1 \text{ is 1} \\ 0^{|x_1|} \cdot g(x_2) \quad \text{otherwise} \end{cases}$

Solution:

(a) $f_a(x) = g(x^c)$ is one-way. Proof by contradiction (We denote complement with an exponent c) . Assume it is not. Then there is a PPT adversary A of f_a with non-negligible success probability. Let us construct a PPT adversary B for g as follows: on input y

- get $z = A(y)$
- return z^c

$$g(B(y)) = g(z^c) = f_a(z) = f_a(A(y))$$

Thus B is successful whenever A is successful. Hence B also has a non-negligible success probability, implying that g is not one-way, a contradiction. Hence f_a is one-way.

(b) $f_b(x) = g(x_1 \oplus x_2)$ is one-way. Proof by contradiction . Assume it is not. Then there is a PPT adversary A of f_b with non-negligible success probability. Let us construct a PPT adversary B for g as follows: on input y

- get $x'_1, x'_2 = A(y)$
- return $x'_1 \oplus x'_2$

$$g(B(y)) = g(x'_1 \oplus x'_2) = f_b(x'_1||x'_2) = f_b(A(y))$$

Thus B is successful whenever A is successful. Hence B also has a non-negligible success probability, implying that g is not one-way, a contradiction. Hence f_a is one-way.

(c) f_c is one-way. Let $|x_1| = |x_2| = n$ and $|x| = 2n$. Proof by contradiction. Assume f_c is not one-way. Then there is a PPT adversary A of f_c with non-negligible success probability. We construct a PPT adversary B for g as follows: On input y,

- Compute $x'_1||x'_2 = x' = A(0^{|y|}y)$
- return x'_2.

$$\begin{aligned} Pr_{x_2}[g(B(g(x_2))) = g(x_2)] &= Pr_{x_2}[g(B(g(x_2))) = g(x_2)|g(x_2) = 0^n].Pr[g(x_2) = 0^n] \\ &+ Pr_{x_2}[g(B(g(x_2))) = g(x_2)|g(x_2) \neq 0^n].Pr[g(x_2) \neq 0^n] \\ &\geq Pr_{x_2}[g(B(g(x_2))) = g(x_2)|g(x_2) \neq 0^n].Pr[g(x_2) \neq 0^n] \end{aligned}$$

When $y = g(x_2)$ is not equal to 0^n, then, as per the definition of f_c, B inverts y whenever A inverts $0^{|y|}y$. Hence,

$$Pr_{x_2}[g(B(g(x_2))) = g(x_2)|g(x_2) \neq 0^n] = Pr[success\ of\ A] \geq \frac{1}{polynomial(2n)} = \frac{1}{polynomial(n)}$$

Further, since g is one-way,

$$Pr[g(x_2)] \neq 0^n \geq \frac{1}{polynomial'(n)}$$

Using these two observations,

$$\begin{aligned} Pr_{x_2}[g(B(g(x_2))) = g(x_2)] &\geq Pr_{x_2}[g(B(g(x_2))) = g(x_2)|g(x_2) \neq 0^n].Pr[g(x_2) \neq 0^n] \\ &\geq \frac{1}{polynomial(n)}.\frac{1}{polynomial(n)} \\ &= \frac{1}{polynomial(n)} \end{aligned}$$

Hence B also has a non-negligible success probability, implying that g is not one-way, a contradiction. Hence f_c is one-way.

(d) f_d is not one-way. Let $|x_1| = |x_2| = n$ and $|x| = 2n$. Let S be the set of all x_1 of length n that have at least one bit as 1. Then $|S| = 2^n - 1$.

Consider the adversary A of f_d that always returns 1^{2n} for any input.

$$
\begin{aligned}
Pr_x[f_d(A(f_d(x))) = f_d(x)] &= Pr_x[f_d(A(f_d(x))) = f_d(x) | x_1 \in S].Pr[x_1 \in S] \\
&+ Pr_x[f_d(A(f_d(x))) = f_d(x) | x_1 \notin S].Pr[x_1 \notin S] \\
&\geq Pr_x[f_d(A(f_d(x))) = f_d(x) | x_1 \in S].Pr[x_1 \in S] \\
&= Pr_x[f_d(1^{2n}) = 0^{2n} | x_1 \in S].\frac{2^n - 1}{2^n} \\
&= Pr_x[0^{2n} = 0^{2n} | x_1 \in S].\frac{2^n - 1}{2^n} \\
&= \frac{2^n - 1}{2^n} \\
&\geq \frac{1}{2}
\end{aligned}
$$

Since A has a significant success probability, f_d is not one-way.

4. (2 points) We know that f may be one way but $f(f(x))$ may not be one way. What about $f(x)||f(f(x))$?

Solution: Yes, $g(x) = f(x)||f(f(x))$ is one-way.

Proof by Contradiction: Assume g(x) is not one-way. There exists a polynomial time randomized attacker A against the one-wayness of g. We construct an attacker B against the one-wayness of f as follows: Upon input of y, B invokes A on input $y||f(y)$. Eventually, A outputs x and B outputs x.

If A runs in polynomial time (in input length n) then B also runs in polynomial time (in input length n). We now show that success in A implies success in B. Let A return a valid inverse x of $y' = y||f(y)$. Therefore, $g(x) = y' = y||f(y)$.

$$\implies f(x)||f(f(x)) = y||f(y) \implies f(x) = y \quad (\textit{on comparing the first parts})$$

Thus success in A implies success in B. This gives that success probability of B is at least as good as that of A. Thus f is not one-way if g is not one-way. But since f is one-way by assumption, we get that $g(x) = f(f(x))$ is one-way.

5. (3 points) Given a strong one way function f, construct a weak one way function g that is NOT a strong one way function.

Solution: We define g as

$$g(x) = \begin{cases} x & , \text{ if } x \mod 2 = 0 \\ f(x) & , \text{ otherwise} \end{cases}$$

(a) To show that there exists an adversary A for g with non-negligible success probability. Let A be

defined as A(y) = y. Success probability of A is

$$\begin{aligned}
Pr_x[g(A(g(x))) = g(x)] &= Pr_x[g(A(g(x))) = g(x)|x\ mod 2 = 0]Pr[x\ mod 2 = 0] \\
&+ Pr_x[g(A(g(x))) = g(x)|x\ mod 2 = 1]Pr[x\ mod 2 = 1] \\
&= \frac{1}{2}Pr_x[g(A(g(x)))=g(x)|x\ mod 2=0] + \frac{1}{2}Pr_x[g(A(g(x))) = g(x)|x\ mod 2 = 1] \\
&= \frac{1}{2}Pr_x[x = x|x\ mod 2 = 0] + \frac{1}{2}Pr_x[g(g(x)) = g(x)|x\ mod 2 = 1] \\
&= \frac{1}{2}.1 + \frac{1}{2}Pr_x[g(g(x)) = g(x)|x\ mod 2 = 1] \\
&\geq \frac{1}{2}
\end{aligned}$$

Hence g is not a strong one-way function.

(b) To show that failure probability of any adversary of g is significant. Proof by contradiction. Assume that there exists a PPT adversary A for g whose failure probability is not significant.

$$Pr[failure of A] \leq neg(n)$$

$$\implies Pr[success of A] \geq 1 - neg(n)$$

We construct a PPT adversary B of f as follows: given input y, return A(y). Success probability of B is

$$\begin{aligned}
Pr_x[f(B(f(x))) = f(x)] &= Pr_x[f(A(f(x))) = f(x)] \\
&= Pr_x[f(A(f(x))) = f(x)|x\ mod 2 = 0]Pr[x\ mod 2 = 0] \\
&+ Pr_x[f(A(f(x))) = f(x)|x\ mod 2 = 1]Pr[x\ mod 2 = 1] \\
&= \frac{1}{2}Pr_x[f(A(f(x)))=f(x)|x\ mod 2=0] + \frac{1}{2}Pr_x[f(A(f(x))) = f(x)|x\ mod 2 = 1] \\
&\geq \frac{1}{2}Pr_x[f(A(f(x))) = f(x)|x\ mod 2 = 1] \\
&\geq \frac{1}{2}Pr_x[g(A(g(x))) = g(x)] \\
&= \frac{1}{2}Pr[Success\ of\ A] \\
&\geq \frac{1}{2}(1 - neg(n)) \\
&\geq \frac{1}{4}
\end{aligned}$$

Since success probability of B is significant, we get the contradiction that f is not one-way. Hence our assumption is wrong. Hence, failure probability of any adversary of g is significant.

From the above two points, we see that g is a weak one-way function.