CS171 HW6

Q1. If f is an OWF, then so as g.

∴ (i) Suppose for contradiction that g is not OWF, so there exists adversary A that can invert g: Given $g(y)$ for some y, A can find x such that $g(x)=g(y)$, i.e. $f(f(x))=f(f(y))$ $f(x)=f(y)$

(ii) We can construct B that uses A to invert f: given $f(y)$ for some y, B computes $g(y)=f(f(y))$ and use A to find x such that $f(x)=f(y)$.

(iii) If g is not OWF, then we can invert f, a contradiction.

Q2. H_3 is not Collision Resistent

∴ Hardness of H_3 is on weaker of H_1 & H_2

Without loss of generity, if A can find $H_2(x')=H_2(x)$, then for the same x' & x, $H_3(x')=H_3(x)$.

~~H_4 is not Collision Resistent~~

~~∴ Without loss of generity, if A can find $H_2(x')=H_2(x)$, then given $Y=f(x)$~~

∴ Without loss of generity, assume H_2 is not collision resistent, but H_2 is.

If adversary A breaks H_4, B can break H_2, a contradiction.

~~If adversary A finds (x_1', x_2') such that~~

H_4 is collision resistent

∴ Without loss of generity, assume H_2 is not collision resistent, but H_2 is.

If adversary A finds x' & x such that $H_4^s(x')=H_4^s(x)$, it finds $H_1^{s_1}(x_1') \| H_2^{s_2}(x_2')=H_1^{s_1}(x_1) \| H_2^{s_2}(x_2)$ from which it can find $H_2^{s_2}(x_2')=H_2^{s_2}(x_2)$ breaking H_2's security, a contradiction.

Q3. ~~If f is not OWF, i.e. invertible, then adversary A can, given $y=f(x)$, find x~~

Suppose for contradiction that f is not OWF, then there exists A, given $y=f(x)$, finds x. Then, B can use A to find this x, and consequently $hc(x)$, breaking hardness of f, a contradiction.

Note this relies on premise that f has a hc Predicate.