VRF Reduction:

Suppose there is an algorithm A having advantage $\epsilon(k)$ in breaking the pseudorandomness of the VRF. We construct an algorithm A' using A to solve the q-DBDHI problem with advantage $\epsilon(k)/2^{q(k)}$ where $q = 2^{q(k)}$. A' is given $(g, g^x, g^{x^2}, \ldots, g^{x^q}) \in G^{q+1}$ and has to distinguish $e(g,g)^{\frac{1}{x}}$ from a random element $\in G_1$. A' will proceed in 4 major steps below:

Step 1: Key_gen:

A': $X_0 \xleftarrow{R} \{0,1\}^{q(k)}$

$Sk = x - X_0$

$P(z) = \prod_{X \neq X_0} (z + X)$

$h = g^{P(Sk)}$

$PK = h^{SK}$

Give A PK

Step 2: Oracle:

$X_1, X_2, \ldots, X_l \leftarrow A^{O.O}(PK)$

A': For i from 1 to l:

If $X_i = X_0$:

$b' \leftarrow \{0,1\}$; Return b'

Else:

$Y_i = e(h,h)^{\frac{1}{Sk + X_i}}$

$\Pi_i = g^{\frac{1}{Sk + X_i}}$

Give A (Y_i, Π_i)