VRF Construction:

Let G and G_1 be two cyclic groups having the same order p, where p is a prime, and $e: G \times G \to G_1$ be a bilinear map. The VRF (Gen, Prove, Ver) is constructed as follow:

$\text{Gen}(1^k)$: $s \xleftarrow{R} \mathbb{Z}_p^*$, $SK = s$, $PK = g^s$

$\text{Prove}(Sk, X)$: $Y = e(g, g)^{\frac{1}{X+Sk}}$

$\pi = g^{\frac{1}{X+Sk}}$

Return (Y, π)

$\text{Ver}(Pk, X, Y, \pi)$: # Check proof:

Check $e(PK \cdot g^x, Y) = e(g, g)$?

Check $Y = \text{Prove}(Sk, X)$

Check $Y = e(\pi, g)$?

Return 1 iff both checks are corre

DBDHI Assumption:

The DBDHI problem: Given $(g, g^x, g^{x^2}, \ldots, g^{x^q}) \in G^{q+1}$ distinguish $e(g, g)^{\frac{1}{x}}$ from a random element $\in G_1$

An algorithm A has advantage ϵ in solving the q-DBDHI problem if:

$|Pr[A(g, g^x, g^{x^2}, \ldots, g^{x^q}, e(g, g)^{\frac{1}{x}}) = 1] - Pr[A(g, g^x, g^{x^2}, \ldots, g^{x^q}, Y) = 1]| \geq \epsilon$

where the probability is taken over $x \in \mathbb{Z}_p^*$ and $Y \in G_1$ and internal coin tosses of A.

VKA

VRF Reduction:

Suppose there is an G_1 in breaking the pseu construct an algori HI problem with adv