Step 3: Challenge:

$X^* \leftarrow A^{O_2}(PK)$

A': If $X^* \neq X_0$:

$b' \xleftarrow{R} \{0,1\}$, Return b'

Else:

$P(z) = (z + X_0)H(x) + \omega$

$T_0 = Y^{\omega^2}$

$T_1 = e(h, g^{\frac{P(SK)-\omega}{X_0+SK}}) e(g^{\omega}, g^{\frac{P(SK)-\omega}{X_0+SK}})$

$= e(g,g)^{\frac{P(SK)^2-\omega^2}{X_0+SK}}$

$Y^* = T_0 T_1$

Give A Y^*

Step 4: Finalize.

$b' \leftarrow A(Y^*)$

A': Return b'

Detailed discription: The reduction uses a similar idea to the VUF reduction of Rabin.

Step 1: Key gen: We choose an X_0 and wish A to use X_0 as the challenge input. Similar to the VUF reduction of Rabin, Micali, Vadhan,, we define $P(z) = \prod_{x \neq X_0} (z +$ and let $h = g^{P(SK)}$, where $SK = x - X_0$, the reason we change the generator like this because we can't calculate $e(g,g)^{\frac{1}{x+SK}}$, but we can calculate $e(h,$ for any $X \neq X_0$, this will be explained later

VIKA