

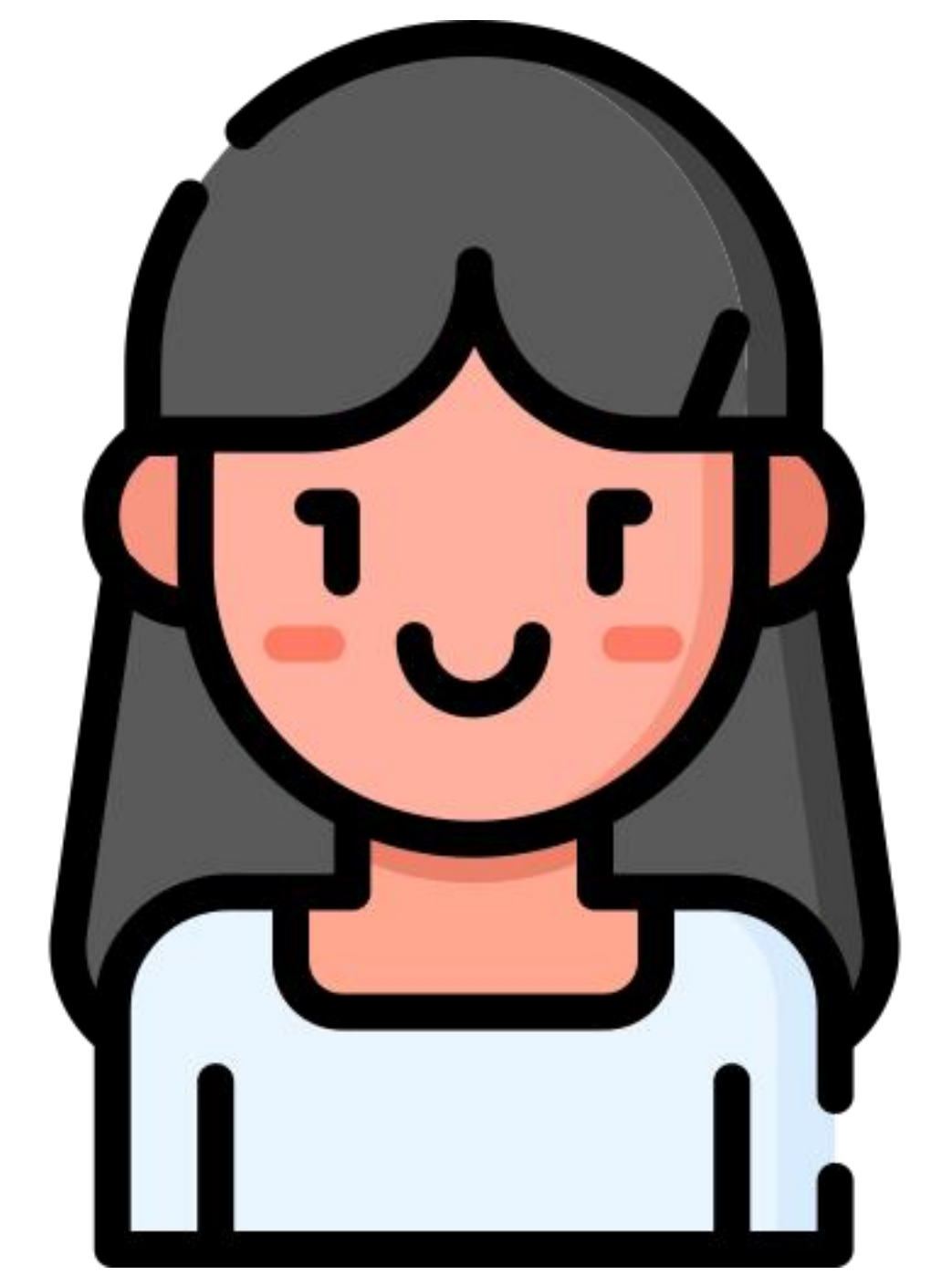
\mathcal{P}



I know w s.t.
 $w^2 = x \pmod{N}$

1. Sample r from \mathbf{Z}_N uniformly
 2. Send $a = r^2 \pmod{N}$
- If I gave you the square root of a and ax , you would be convinced that the claim is true, but you learn the witness w .
 - Instead, I will send you either r or rw , but you are to choose!

\mathcal{V}



Is x indeed a
quadr. residue?



Ok, I choose random bit b

- If $b=0$, send $z = r$
- If $b=1$, send $z = rw \pmod{N}$



Check if $z^2 = ax^b$