ZERO KNOWLEDGE PROOF
IN A NUTSHELL

Peggy knows a secret. She wants to convince Victor she knows the secret without giving away any information at all about the secret.

The Zero Knowledge Proof consists of a series of questions (asked by Victor) and answers (by Peggy) that give zero information about Peggy's secret to Victor. The more questions Peggy answers correctly, the more convinced Victor becomes that Peggy knows the secret.

Example:

Peggy has two balls. They are completely identical in all aspects except for the fact that one is red and the other is green. Victor is color-blind. Peggy wants to prove to Victor that she is not color blind and knows which ball is red and which ball is green.

Victor holds each ball in one hand and shows them to Peggy. He then puts both hands behind his back. Next, he randomly either switches the balls between his hands or leaves them be and then brings them out from behind his back. He asks Peggy to tell him if the balls were switched or not.

Since Peggy is not color-blind she can answer correctly even if the above sequence is repeated many times. Eventually Victor will be convinced Peggy knows which ball is red and which ball is green.

• *No matter how many times the sequence is repeated Victor gains zero knowledge about which ball is red and which ball is green.*

see Fiat-Shamir Zero Knowledge protocol on the next page ⟶

Fiat-Shamir Zero Knowledge Proof:

Public Info: $\boxed{n = pq}$ where p, q are large primes which are kept secret. $\boxed{1 < a < n}$ where $\text{GCD}(a, n) = 1$.

Peggy's Secret $\boxed{1 < s < n}$ where $s^2 \equiv a \pmod{n}$.

- *Peggy wants to prove to Victor that she knows s.*

Peggy chooses random $1 < r_1 < n$ and then $1 < r_2 < n$ such that

$$r_1 \cdot r_2 \equiv s \pmod{n}.$$

She sends $a_1 \equiv r_1^2 \pmod{n}$ and $a_2 \equiv r_2^2 \pmod{n}$ to Victor. Then Victor checks that

$$a_1 a_2 \equiv a \pmod{n}.$$

Victor randomly asks only one of the following two questions:

Question (1) *What is the square root of* $a_1 \pmod{n}$?

Question (2) *What is the square root of* $a_2 \pmod{n}$?

Peggy knows the answer to question (1) is r_1 and the answer to question (2) is r_2. She can always answer correctly. The sequence is repeated (with different random pairs (a_1, a_2) chosen by Peggy) until Victor is convinced Peggy knows s. Victor gains zero knowledge about s during this question and answer process assuming it is infeasible to factor n and the pairs (a_1, a_2) chosen by Peggy are truly random.

- *If the malicious imposter Eve is pretending to be Peggy then Eve can pick $1 < k < n$ with $GCD(k, n) = 1$ and then choose $a_1 \equiv k^2 \pmod{n}$. Eve can find a_2 where $a_1 \cdot a_2 \equiv a \pmod{n}$. Then Eve will be able to answer Qestion (1), but she will not be able to answer Question (2). So, she will give wrong answers about 50% of the time.*