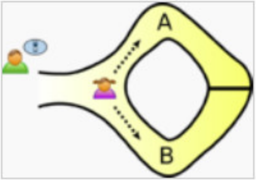
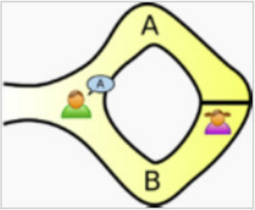
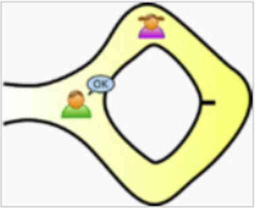
Zero Knowledge Proof (of Knwoledge)



Peggy randomly takes either path A or B, while Victor waits outside



Victor chooses an exit path



Peggy reliably appears at the exit Victor names

Zero-Knowledge (ZK) interactive proof systems

ZK protocols

Who? A **prover** P, a **verifier** V, and sometimes a trusted party sf T
What? P wants to convince V of the truth of an assertion without revealing a full answer.
How? P and V exchange multiple messages, usually dependent on random numbers.

Properties - Intuition

- **Completeness:** A interactive (proof) protocol is complete if given an honest prover P and an honest verifier V the protocol succeeds with overwhelming probability.
- **Soundness:** If the statement is false, no cheating prover $P = \mathcal{A}$ can convince the honest verifier V that the assertion is true (except with negligible probability).
- **Zero knowledge:** Implies that an honest prover P executing the protocol does not release any information about its secret knowledge other than that the particular assertion is true.

Σ protocols

Σ protocols

Protocols which have the above three-move structure:

1. *commitment*
2. *challenge*
3. *response*

are called **sigma protocols** (Σ-protocols).

Example of Σ-protocols are *Fiat-Shamir* and *Schnorr* Zero Knowledge (ZK) protocols.

Fiat-Shamir Protocol

One-time setup

- A trusted party Ted publishes an RSA-like modulus $N = pq$ but keeps the primes p, q private.
- Peggy chooses a number $x \in \mathbb{Z}_N^*$ (i.e. x is relatively prime to N) and computes $X = x^2 \mod N$. Peggy's secret key is x and her public key is $X \in \mathbb{Z}_N$ as her public key.

Iterative Protocol

Iterate the following protocol t times. Victor (V) acts as verifier and accepts Peggy's (P) proof if and only if all the t rounds succeed:

1. P chooses random commitment $r \in \mathbb{Z}_N$ and sends the witness witness $R = r^2 \mod N$ to V.
2. V randomly chooses a challenge $b \in \{0, 1\}$ and sends b to P.
3. P computes proof $Z = r \cdot x^b \mod N$ and returns Z to V.
4. V checks the proof Z in the following way: if $Z^2 = R \cdot X^b \mod N$ holds, than it accepts Z, otherwise V rejects Z.

Analysis of the Fiat-Shamir protocol

Attack against Fiat-Shamir

- If P does not know x, she can produce good values if she can *predict* b.
  How? P can choose a random proof $Z \in \mathbb{Z}_N$ and generate the witness R according to the value of b:

$$\text{if } b = 0, \text{ set } R = Z^2 \in \mathbb{Z}_N,$$
$$\text{if } b = 1, \text{ set } R = Z^2 \cdot X^{-1} \in \mathbb{Z}_N.$$

Consequence: at each round of the protocol someone pretending to be P has probability $\frac{1}{2}$ of fooling V, assuming that V chooses $b \in \{0, 1\}$ with equal probabilities. By iterating the protocol t times, the probability of a false P being accepted is reduced to 2^{-t}.

Is it secure?

What does V (or a listening Adversary) **learn** about P's **secret** x from the protocol run?

Nothing! x is always hidden since it is multiplied with an *unknown random* number.
Security of Fiat-Shamir protocol is based on difficulty of extracting **square roots** (retrieving x from the public key $X = x^2 \mod N$) modulo large composite $N = pq$ (of which the factorisation is unknown to the adversary).