CSCI361

Fair Exchange and Zero Knowledge Proofs

Fair Exchange

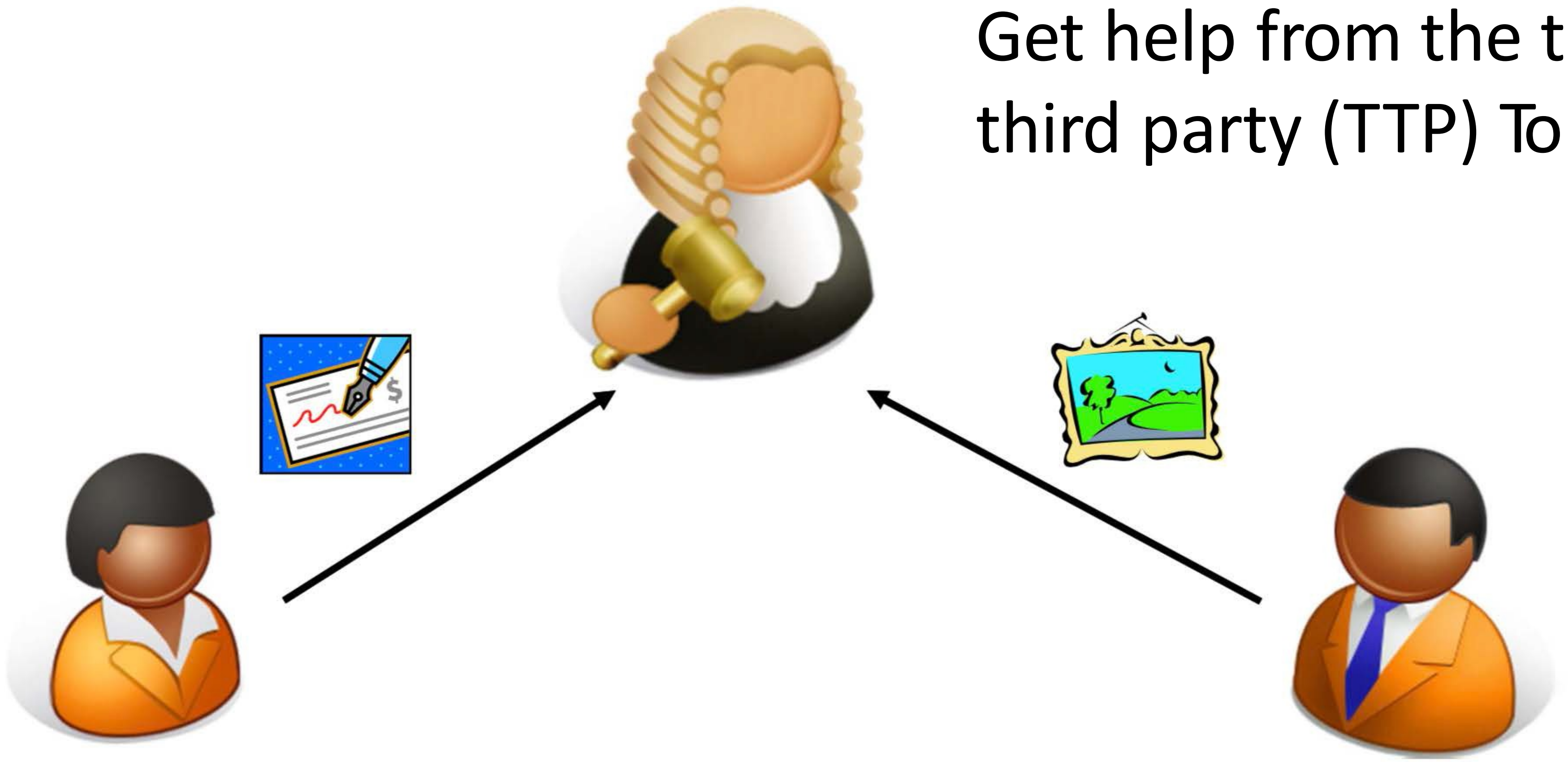
- Two parties, Alice and Bob, would like to exchange something

Let’s say Alice wants to get a digital photo from Bob and Bob wants to get Alice's eCheque (which Alice signed) in exchange. We want to make sure that this transaction is fair.

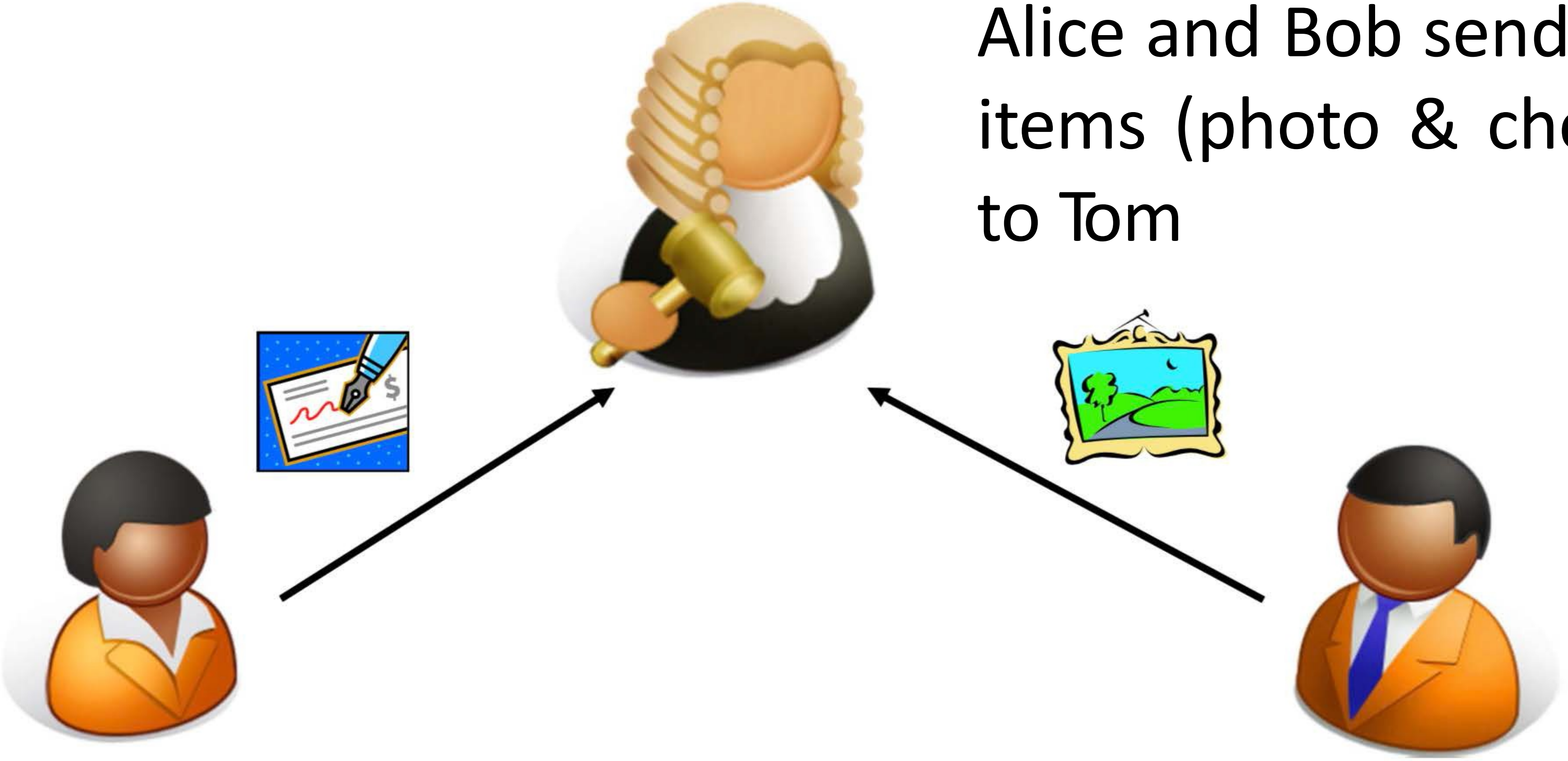
- What is fairness then?
  - ➢ (In the context of electronic commerce), Participants shouldn’t have advantages over each other.
  - ➢ For example: It wouldn’t be fair if one party can avoid their obligations in a contract if the other party has completed their obligations in a contract.

Possible Solution

Get help from the trusted third party (TTP) Tom!



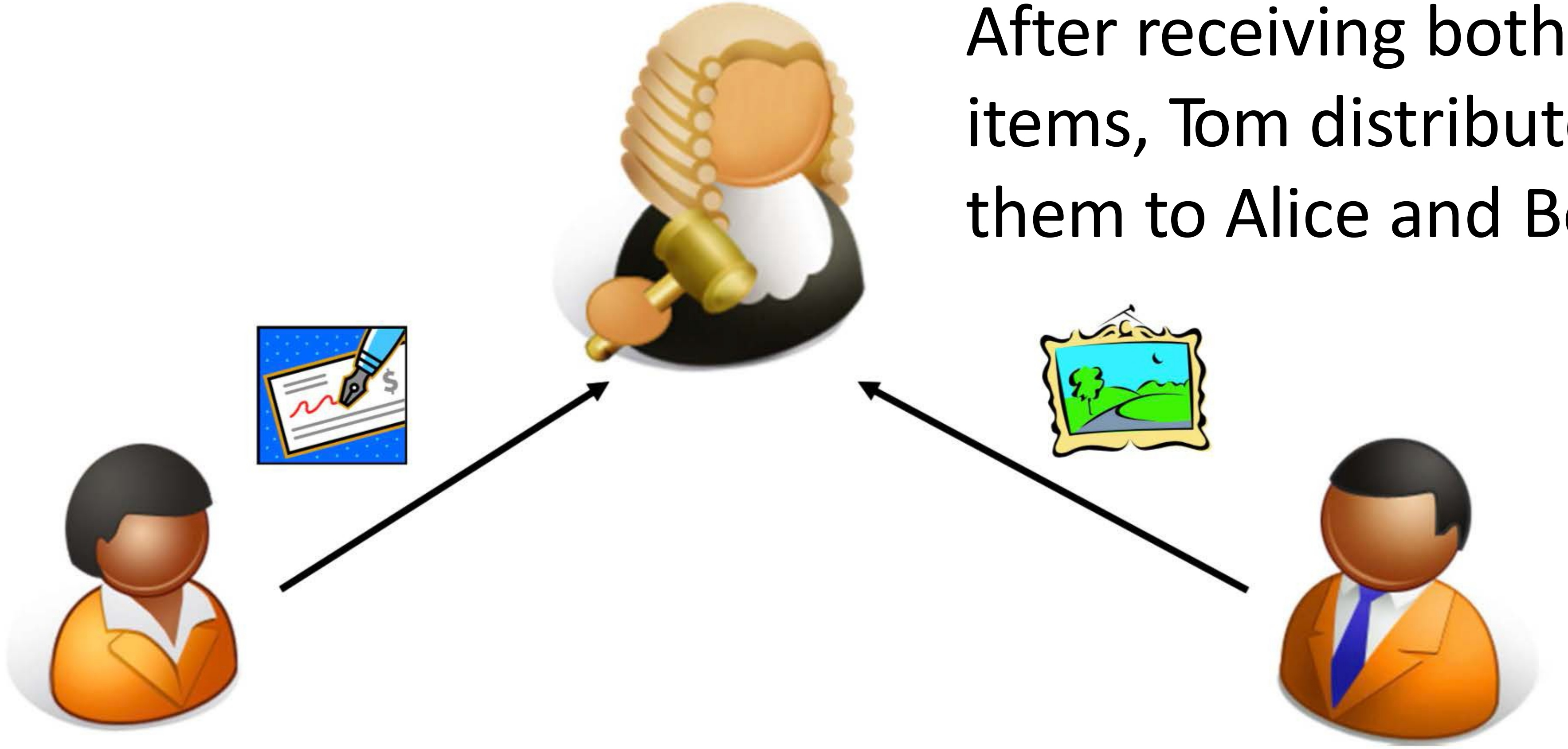
Possible Solution



Alice and Bob send their items (photo & cheque) to Tom

Possible Solution

After receiving both items, Tom distributed them to Alice and Bob



Good…

- But Tom must be accessible all the time
- Can Alice and Bob conduct the exchange without the *active* participation from Tom? (Tom has to receive and send something from Alice and Bob.)

Optimistic Fair Exchange

Scenario: Alice wants to get a digital item from Bob and Bob wants to get Alice's signature in exchange.

- (Conceptual) <u>Solution</u>

➢ Alice creates something called a partial signature (P)

➢ Alice sends P to Bob.

➢ Bob sends Alice his item.

➢ Alice sends her full signature (S) to Bob

  ❖ <u>If Alice runs away after getting Bob's item, Bob can go to Tom and asks Tom to convert P into S</u>.

Optimistic Fair Exchange - Realisation

1. Alice generates her signature, S_A.
2. Instead of sending S_A directly to Bob, Alice encrypts S_A under Tom's public key. The resulting ciphertext $P = E_{pk}(S_A)$ is the partial signature.
3. Alice sends P to Bob.
4. Bob sends his item to Alice.
5. Alice sends S_A to Bob.
   – If Alice does not send S_A to Bob, Bob can contact Tom with P and ask him to decrypt P to S_A. (Bob can finally obtain S_A.)

Optimistic Fair Exchange - Realisation

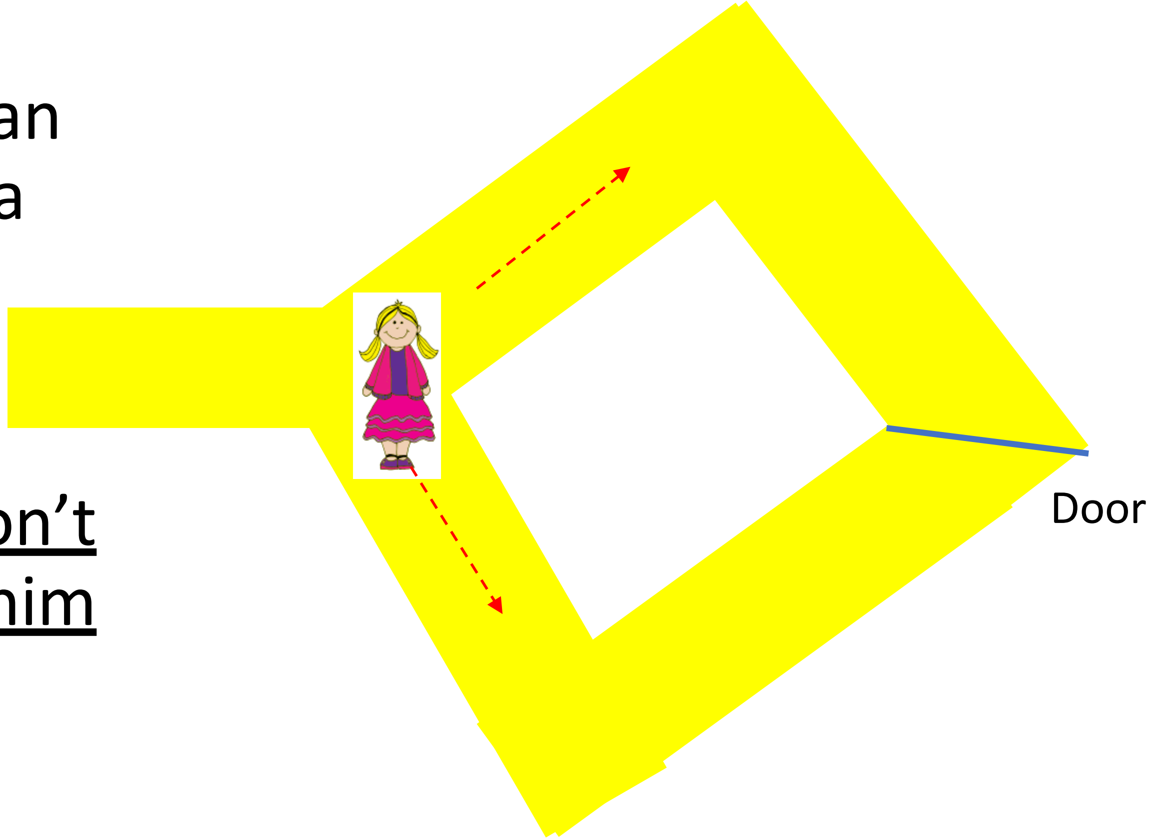
- Additional step
  - ✓ How can Bob make sure C contains a valid signature of Alice?
  - ✓ Using zero-knowledge proof → Prove that P is the encryption of a valid S_A without revealing S_A

Beyond Optimistic Fair Exchange

- Optimistic Fair Exchange can solve the problem of having to require active TTP
- There is a Fair Exchange scheme that does not require TTP at all!

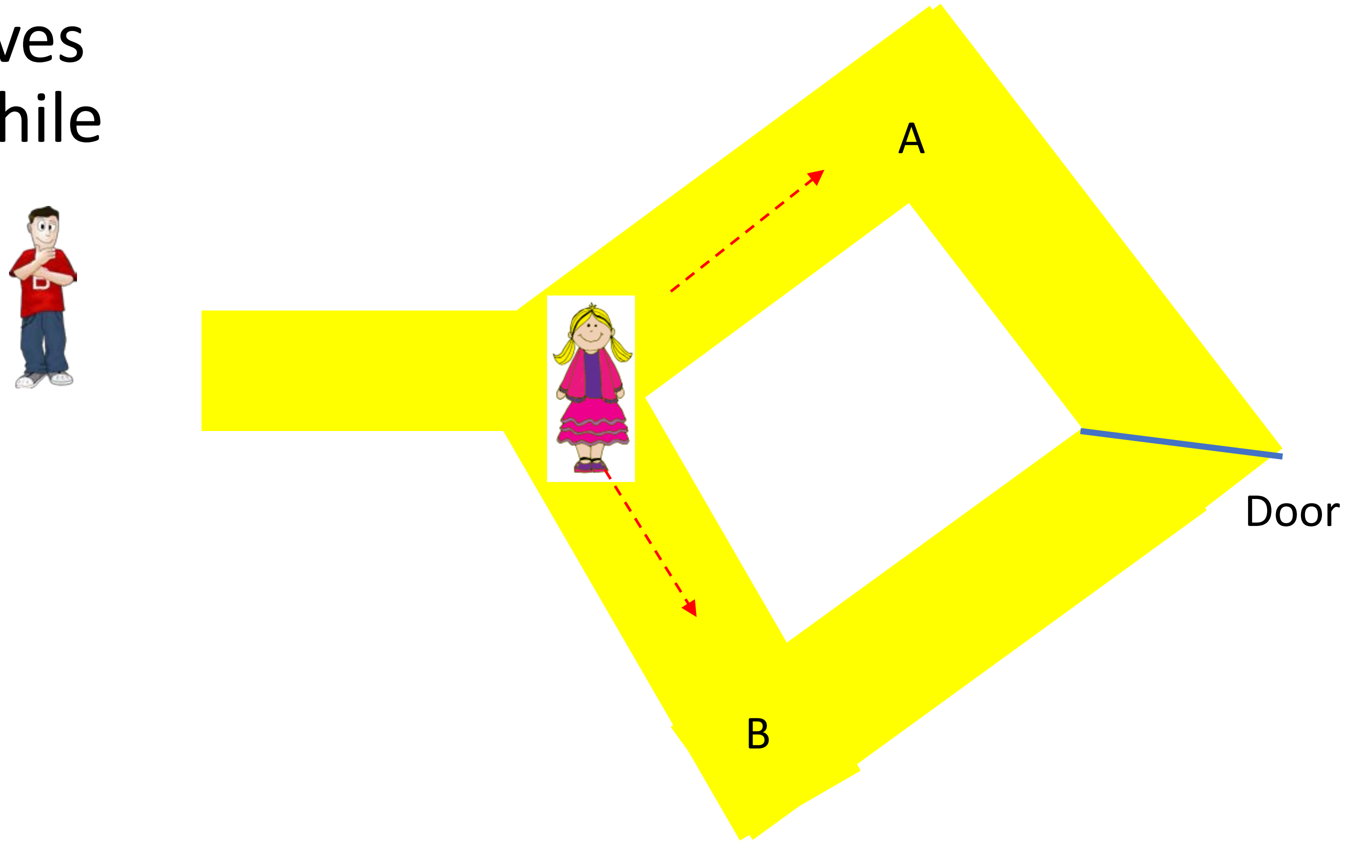
Zero Knowledge Proof: Ali Baba Cave Problem

- Setting: There is a ring-shape cave where the path is blocked by a door. Peggy can open the door if she uses a right magic word as a key. Victor wants to know whether Peggy knows the magic word. <u>But Peggy won't reveal the magic word to him</u> (or anyone else).



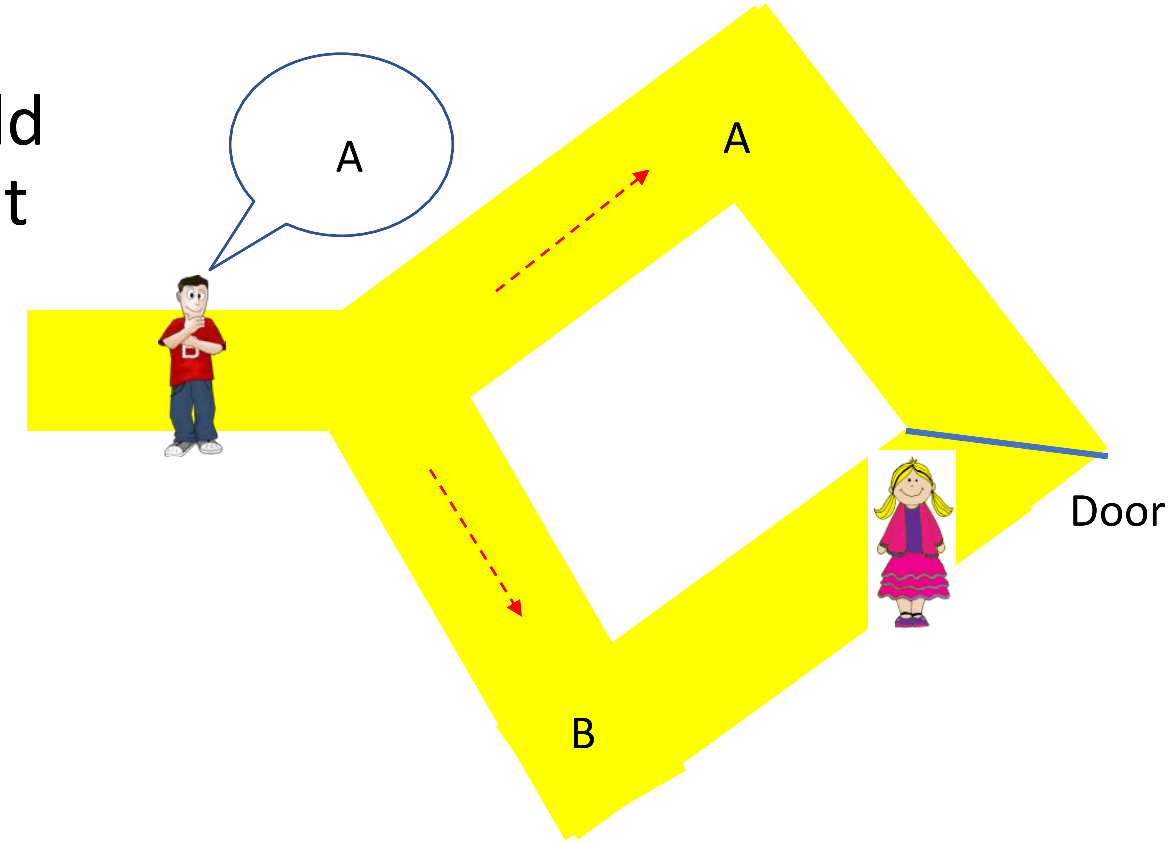
Zero Knowledge Proof: Ali Baba Cave Problem

- Step 1: Peggy chooses either path A or B and moves towards the door while Victor waits outside



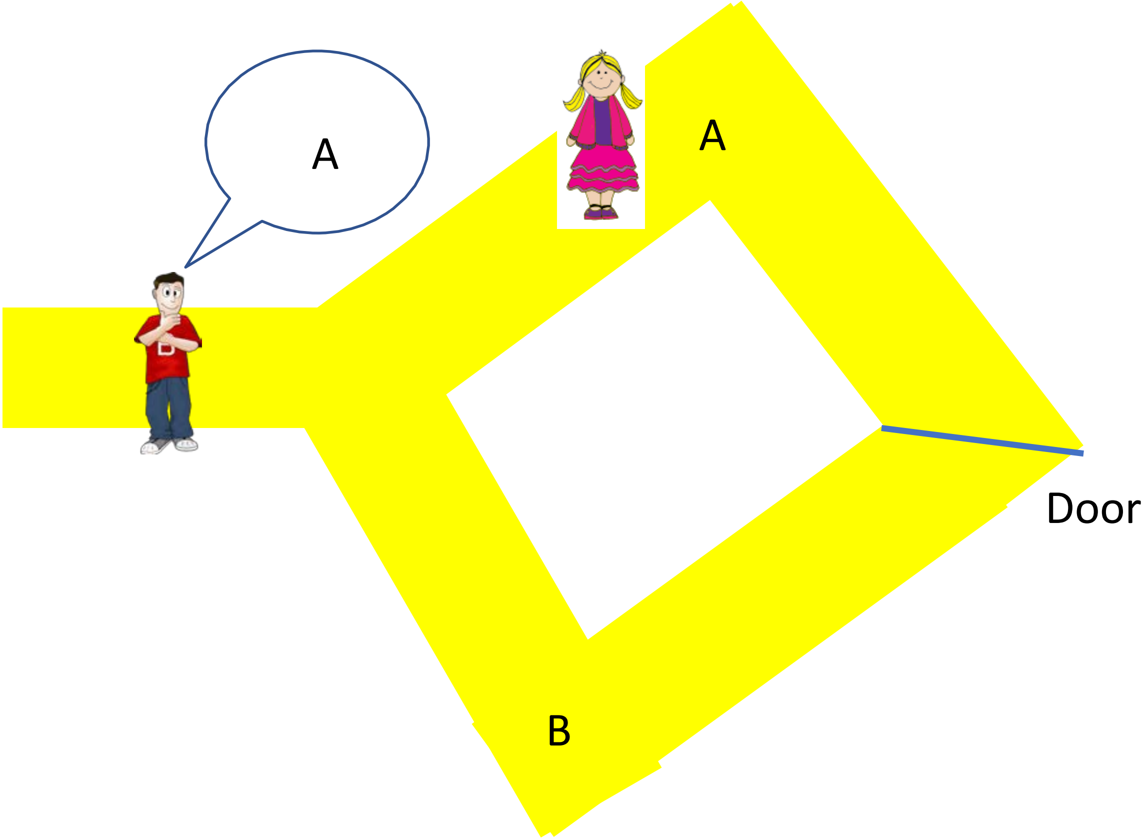
Zero Knowledge Proof: Ali Baba Cave Problem

- Step 2: Now Victor enters the cave, picks at random the name of path Peggy should use to return and shouts it out!



Zero Knowledge Proof: Ali Baba Cave Problem

- Step 3: Peggy returns to the entrance using the path Victor named



Zero Knowledge Proof: Ali Baba Cave Problem

- If Peggy knows the magic word, she can reliably return to the entrance using the path Victor named
- If Peggy does not know the magic word, she can return to the entrance only if Victor named the path she chose in Step 2 with probability ½
- Victor repeat Step 1 to 3 many times to see whether Peggy really knows the magic word
  - In n trials, the probability that Peggy returns through the path without knowing the magic word is $(1/2)^n$