Make noise and whisper: a solution to relay attacks

Omar Choudary and Frank Stajano

Computer Laboratory
University of Cambridge

Mafia relay attack

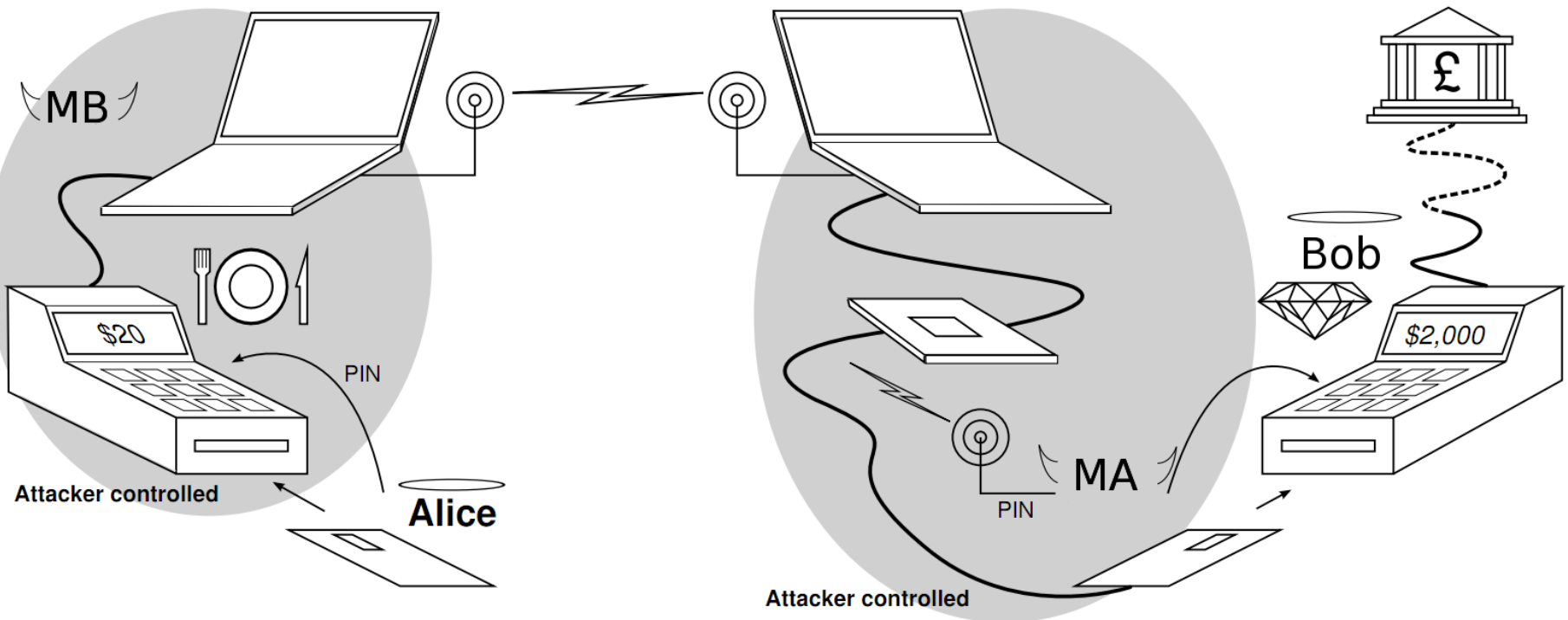


Image adapted from *"Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks"*, Saar Drimer and Steven Murdoch

Mafia relay attack - implemented

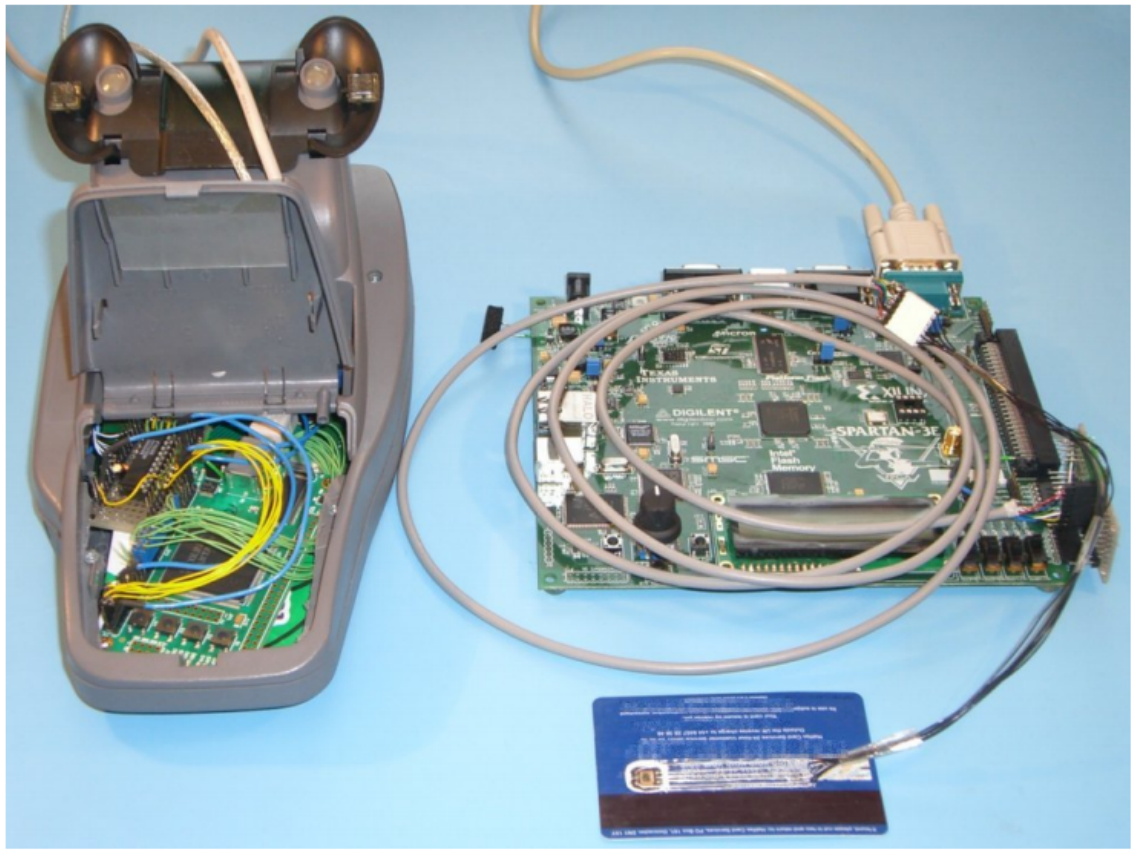


Photo from *"Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks"*, Saar Drimer and Steven Murdoch

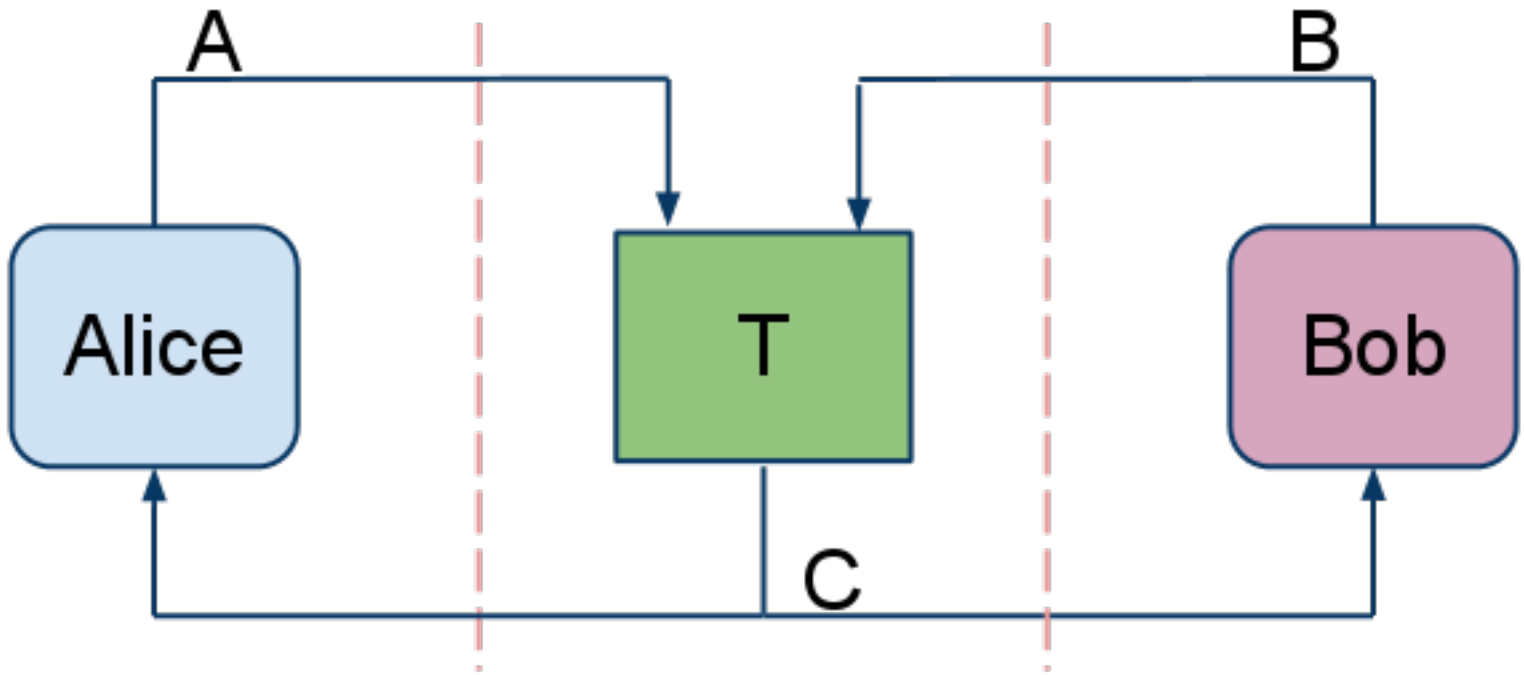
Existing solutions: distance-bounding

round-trip time Alice - MB

VS

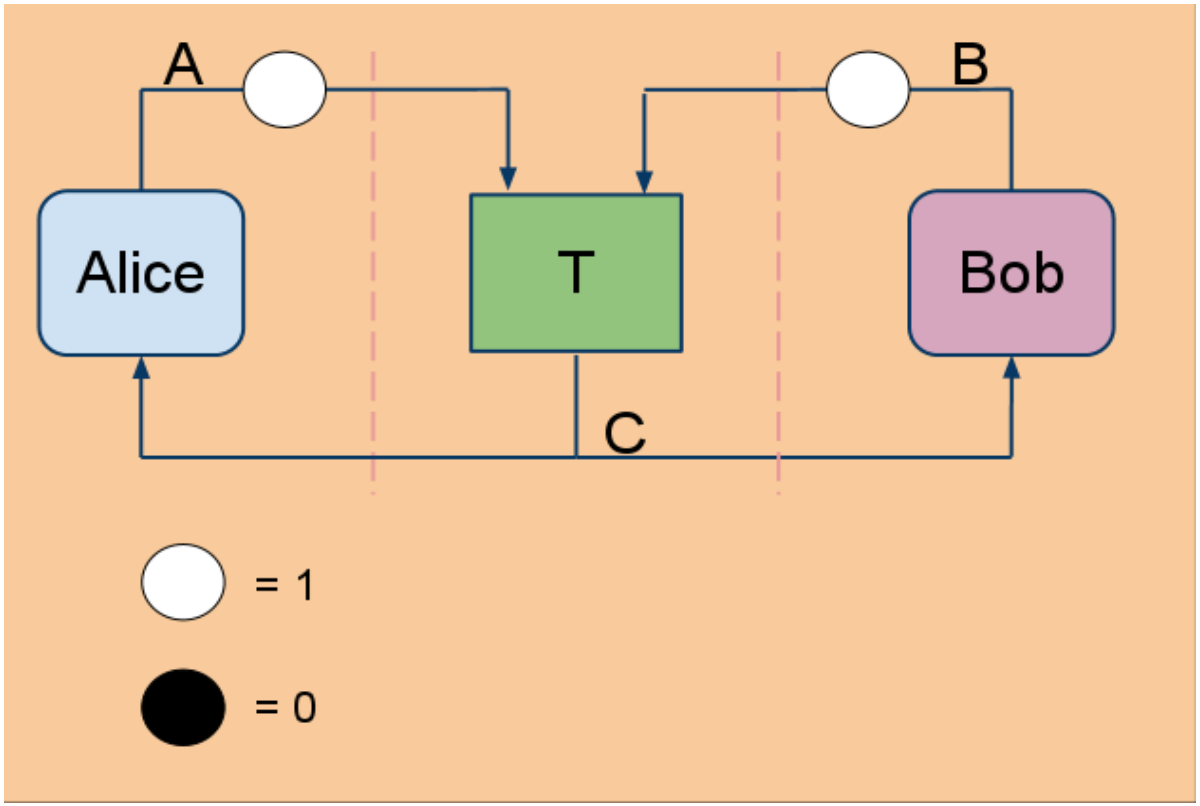
round-trip time Alice - Bob

Our solution: noise-based



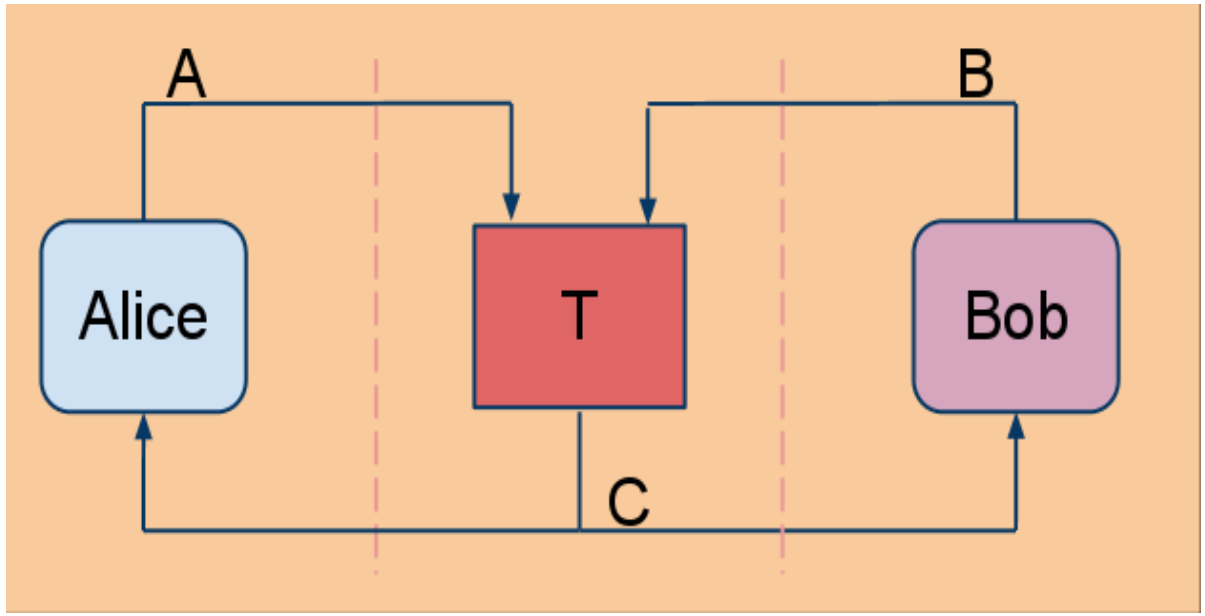
- Bob introduces errors on **some** of Alice's bits
- Alice can see **some** of Bob's errors
- Alice and Bob share a secret key

Our solution: how it works (case 1)



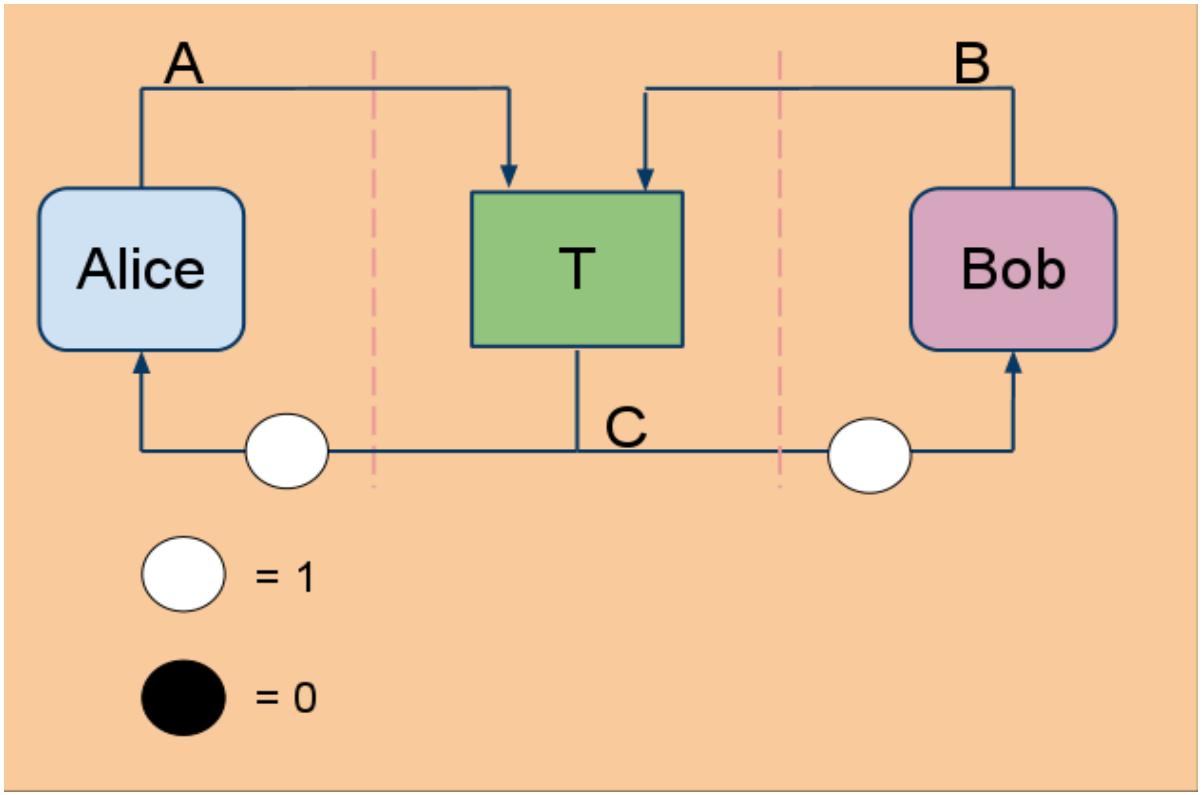
- Bob doesn't introduce any errors
- Once Alice and Bob have sent their bit, they can't modify it

Our solution: how it works (case 1)



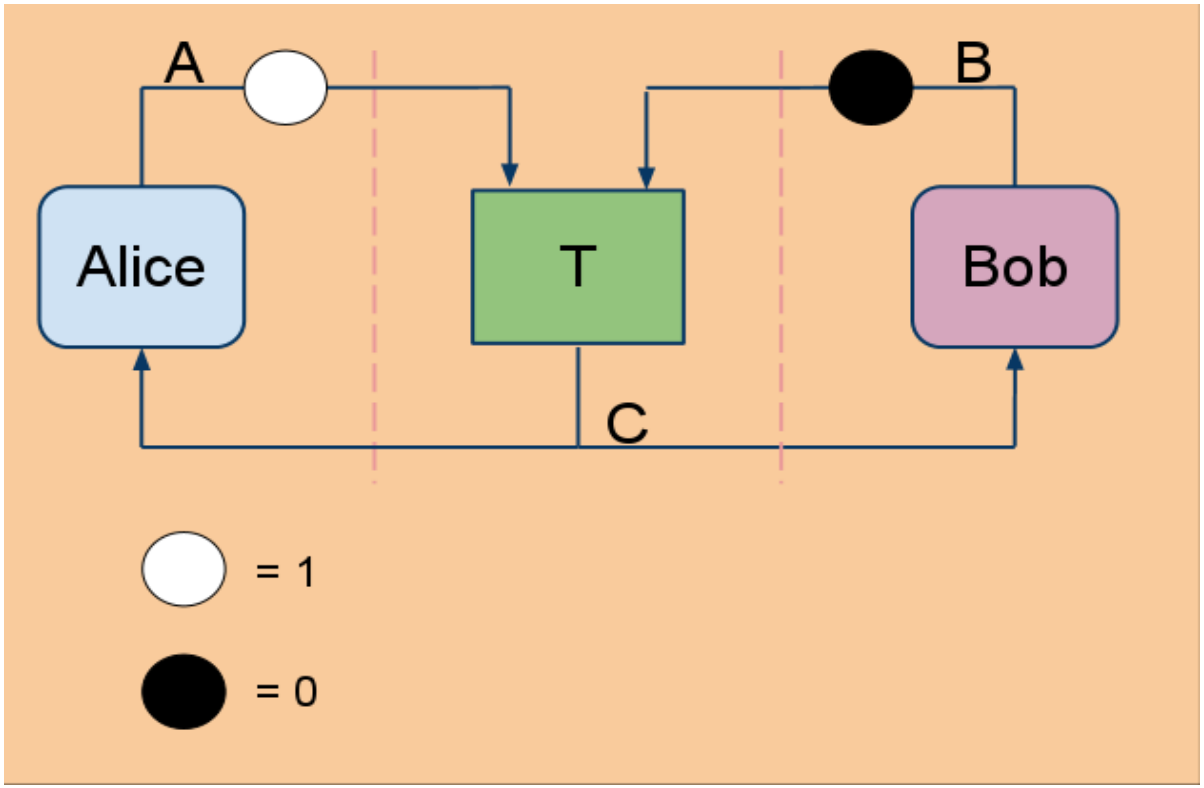
- The T box computes the output and ensures that neither Alice or Bob can see the other's input

Our solution: how it works (case 1)



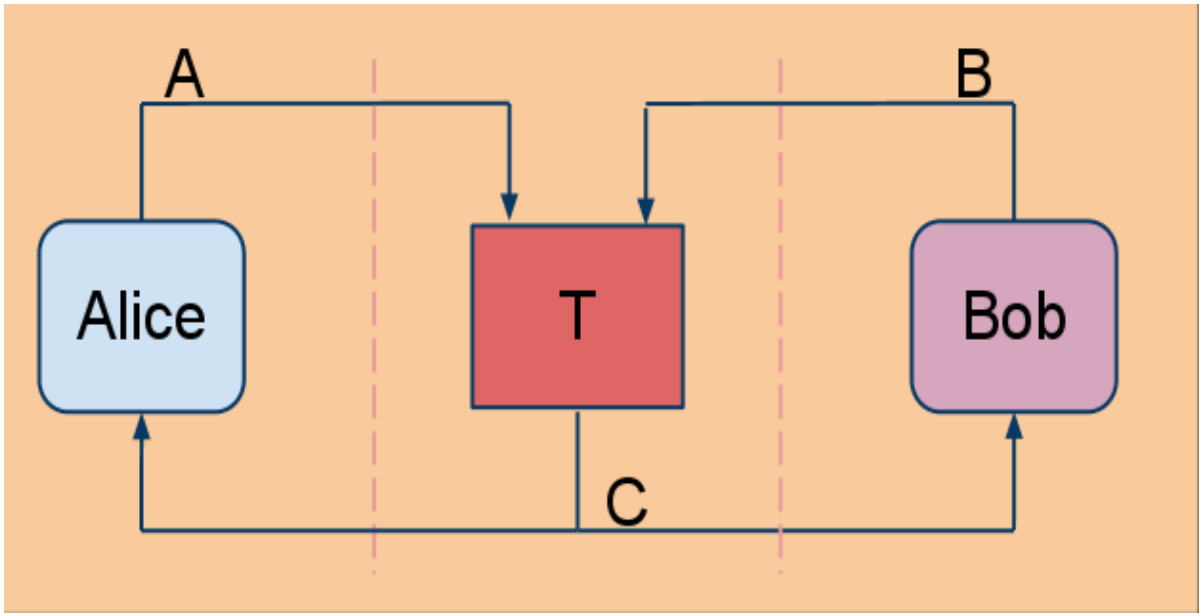
- Both Alice and Bob see the same output

Our solution: how it works (case 2)



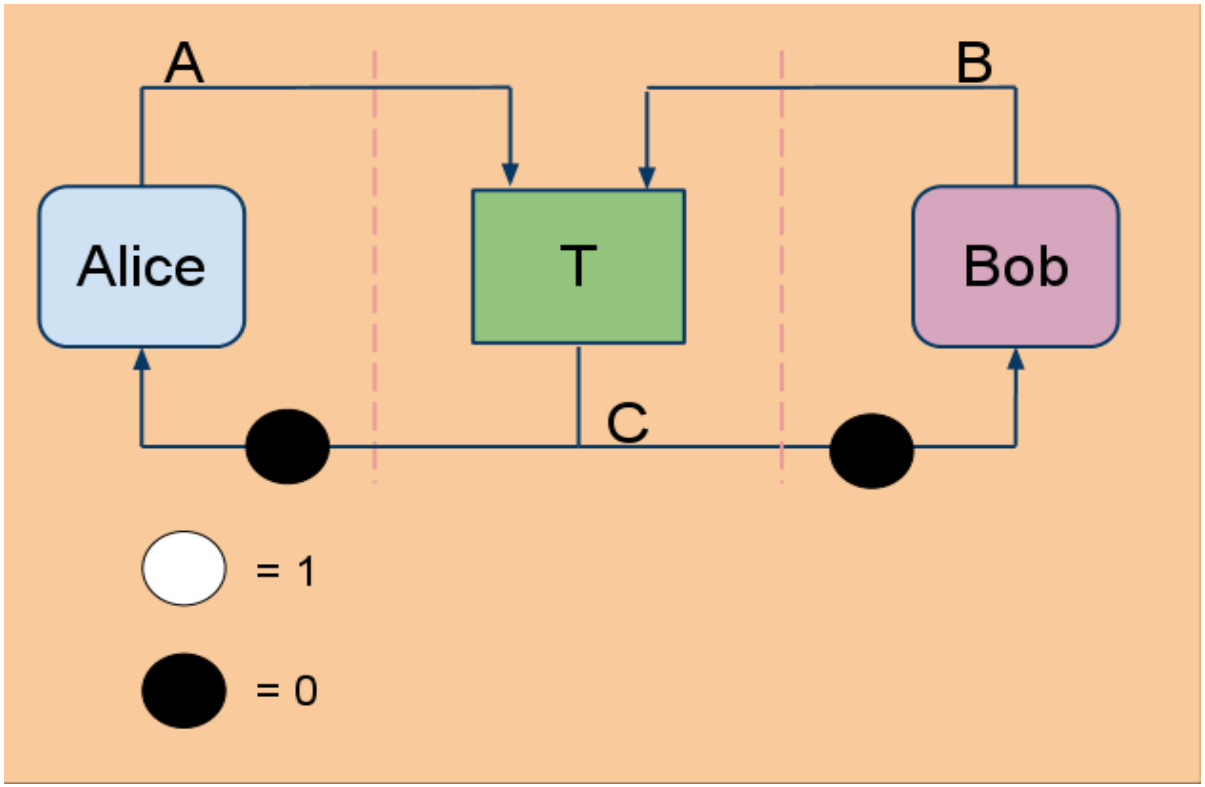
- Bob introduces error
- Once Alice and Bob have sent their bit, they can't modify it

Our solution: how it works (case 2)



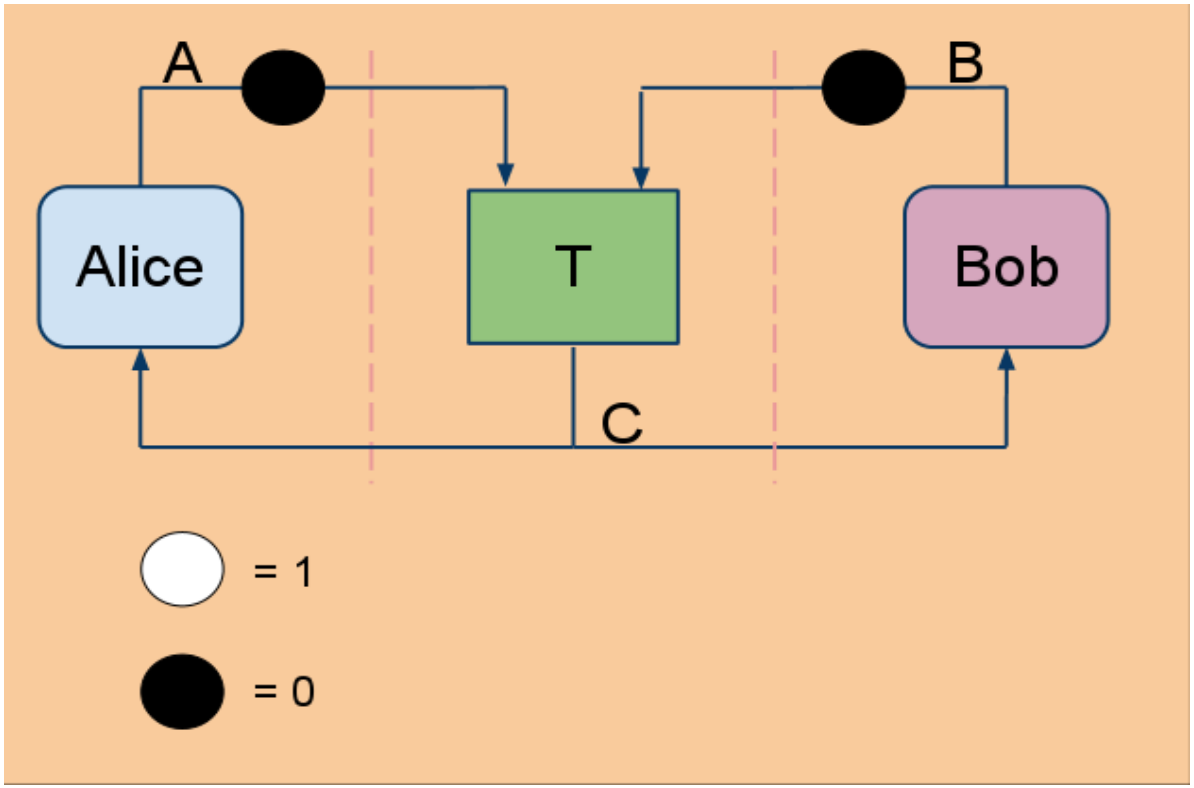
- The T box computes the output and ensures that neither Alice or Bob can see the other's input

Our solution: how it works (case 2)



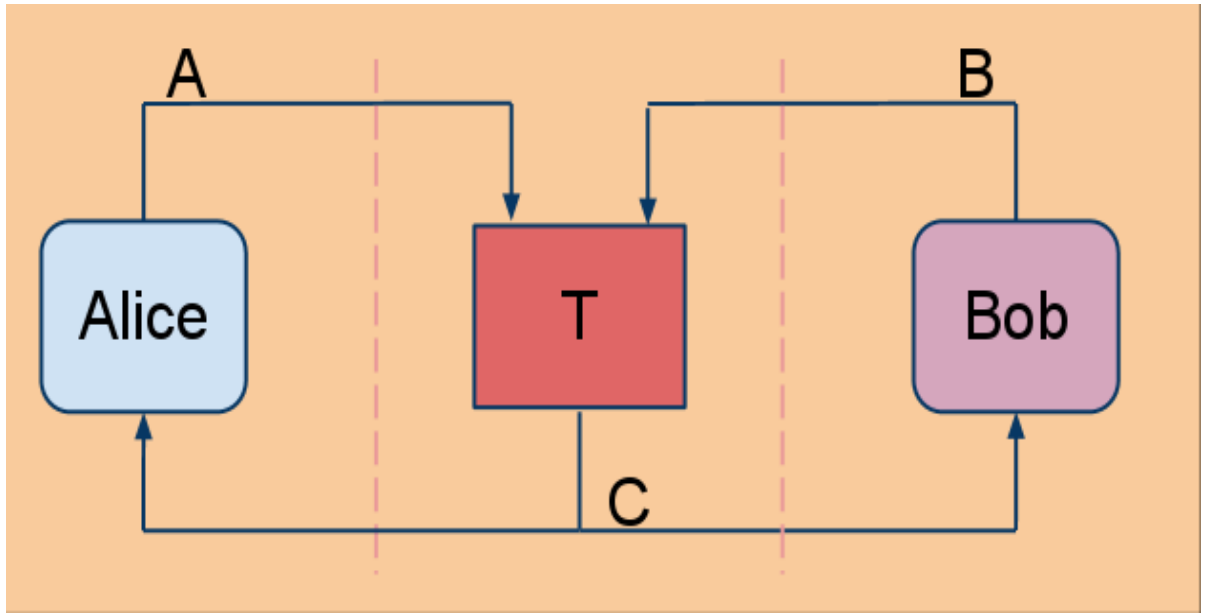
- The output is different than Alice's input so she observes Bob's error
- Bob cannot determine Alice's input

Our solution: how it works (case 3)



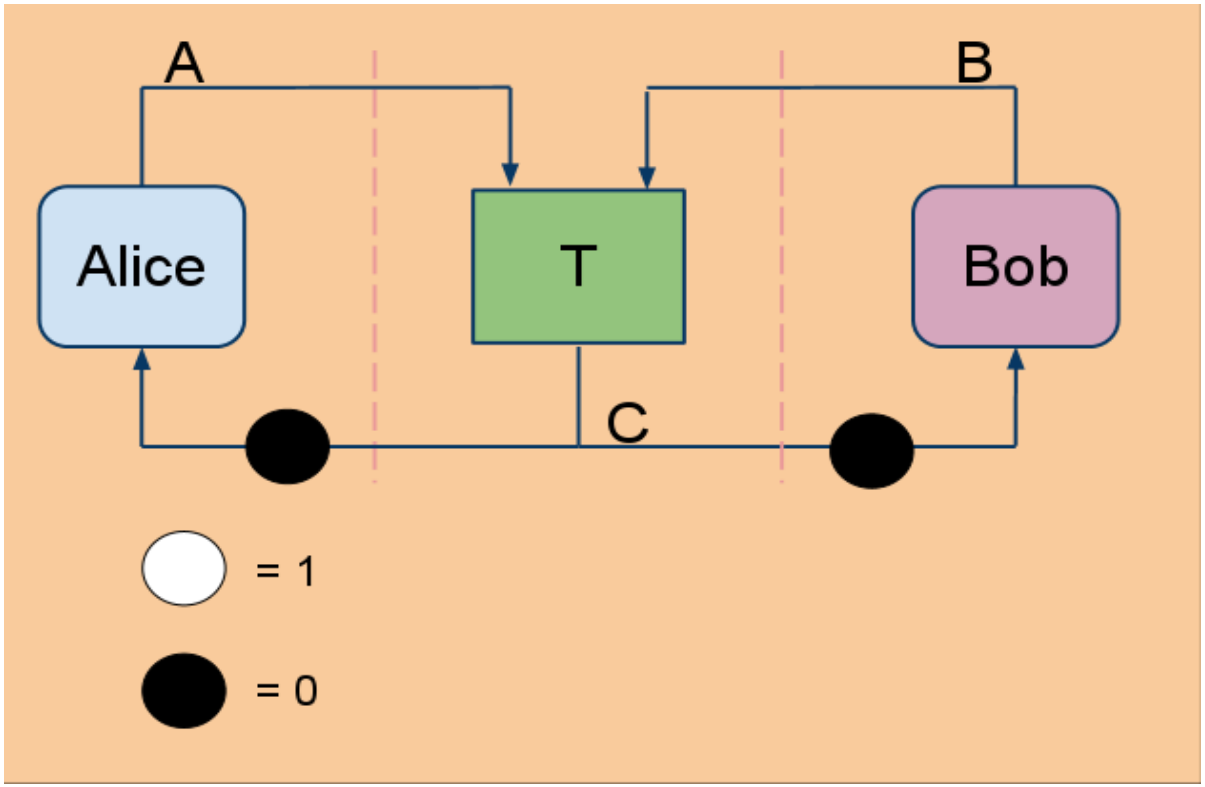
- Bob introduces error
- Once Alice and Bob have sent their bit, they can't modify it

Our solution: how it works (case 3)



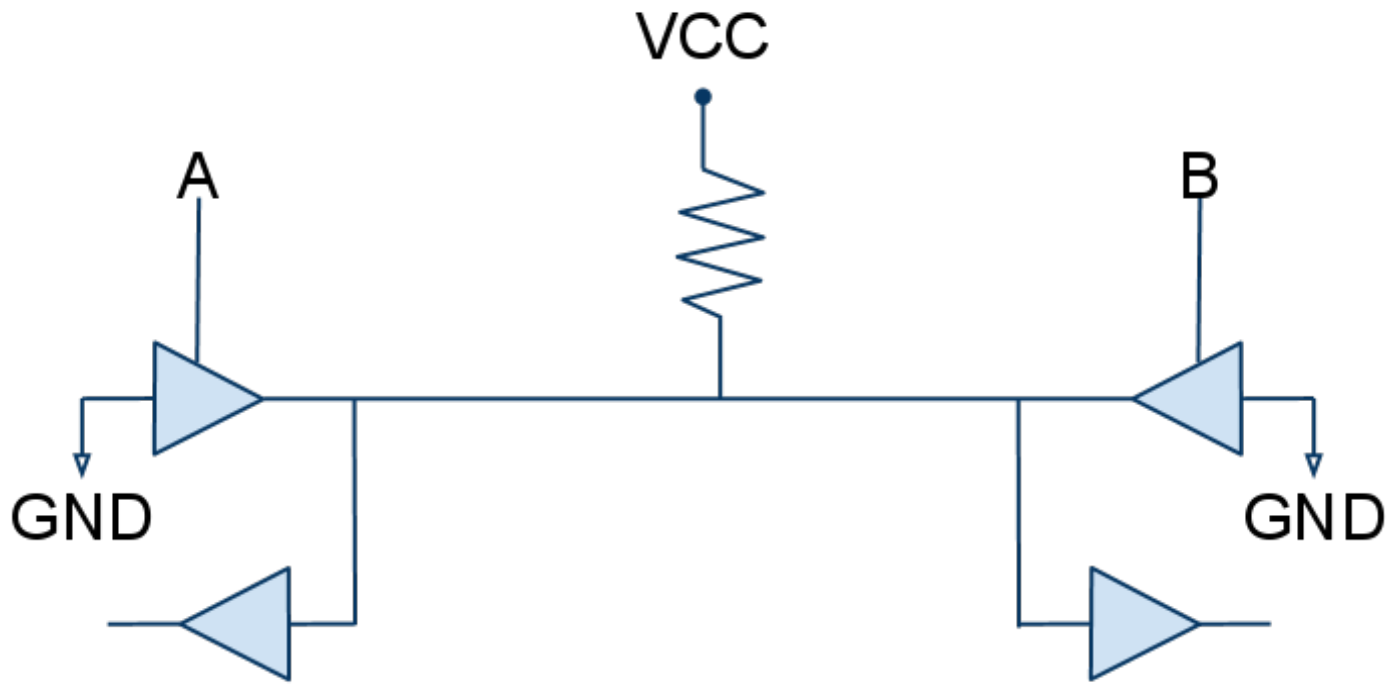
- The T box computes the output and ensures that neither Alice or Bob can see the other's input

Our solution: how it works (case 3)



- Bob cannot determine Alice's input, AND
- Alice cannot observe if Bob has introduced an error, since the output is the same as her input

Implementation - example 1

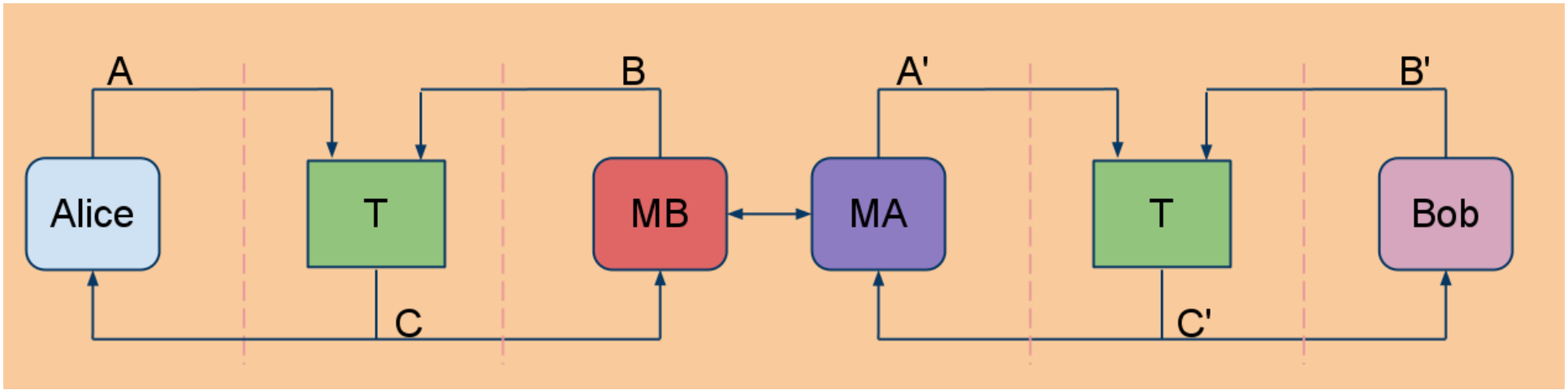


- Bidirectional channel, e.g. ISO 7816
- Alice and Bob can send 0 (GND) or 1 (pull-up resistor)

Implementation - example 1

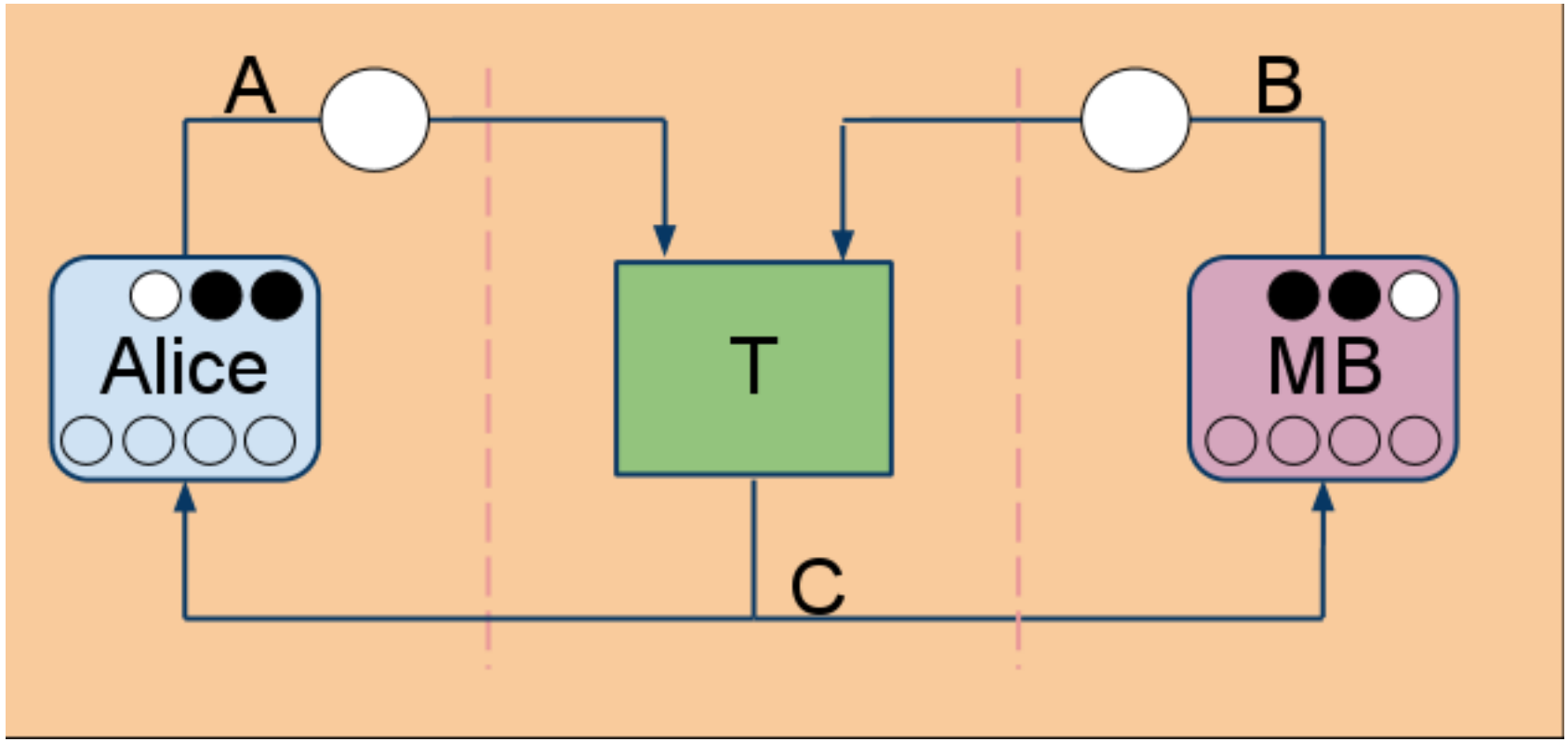
- Protocol:
  - Alice and Bob share a secret key
  - For i=1,N
    - A -> B: R_K[i]
    - Bob introduces errors in 50% of bits
  - At the end of the run, Bob sends the N bits received to Alice
  - Alice compares the number of correct bits with the number she expected
  - if a pair of attackers were involved this should be detectable

Our solution: detect a relay attack



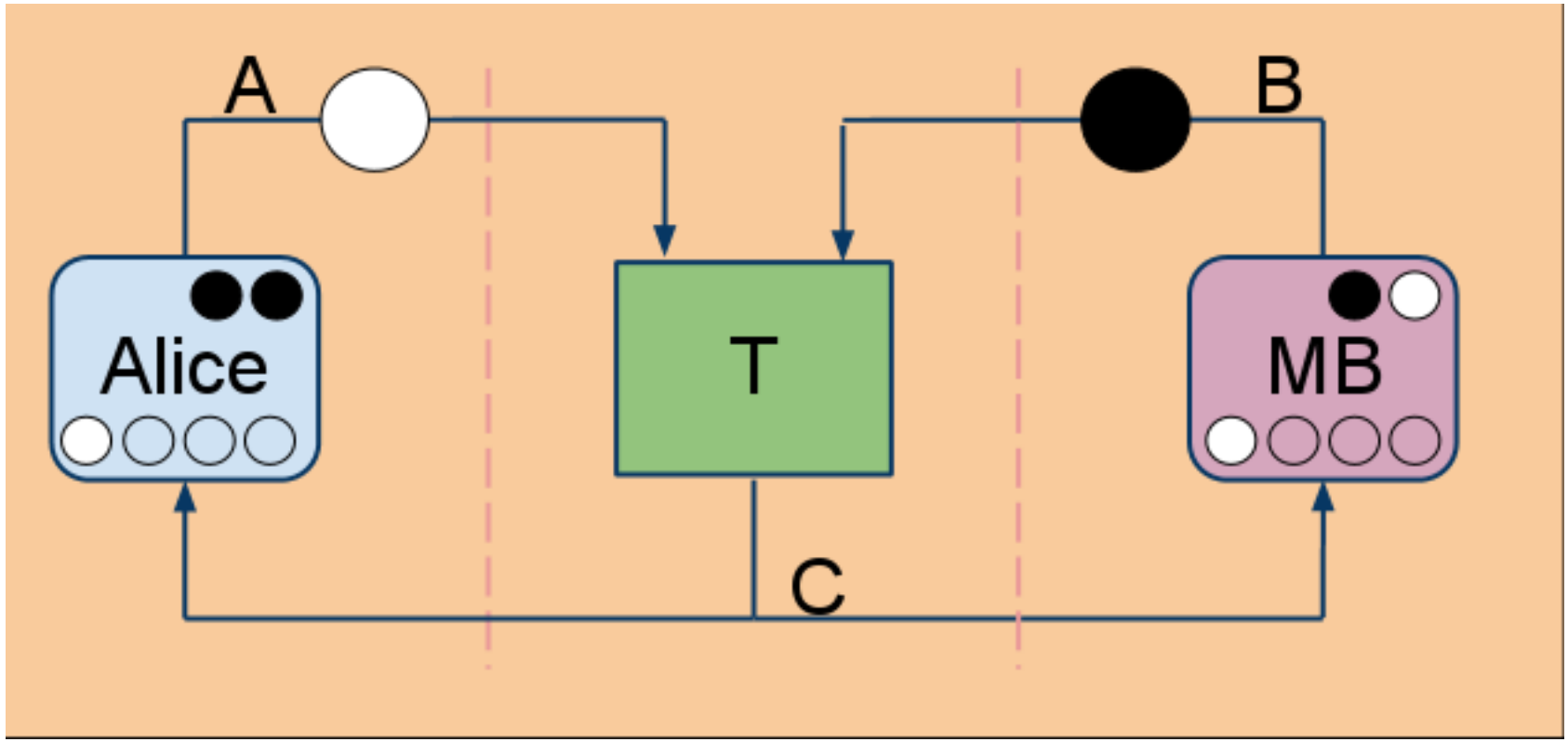
- MA and MB can relay data on perfect channel
- But they are constrained by the T box

Our solution: detect a relay attack



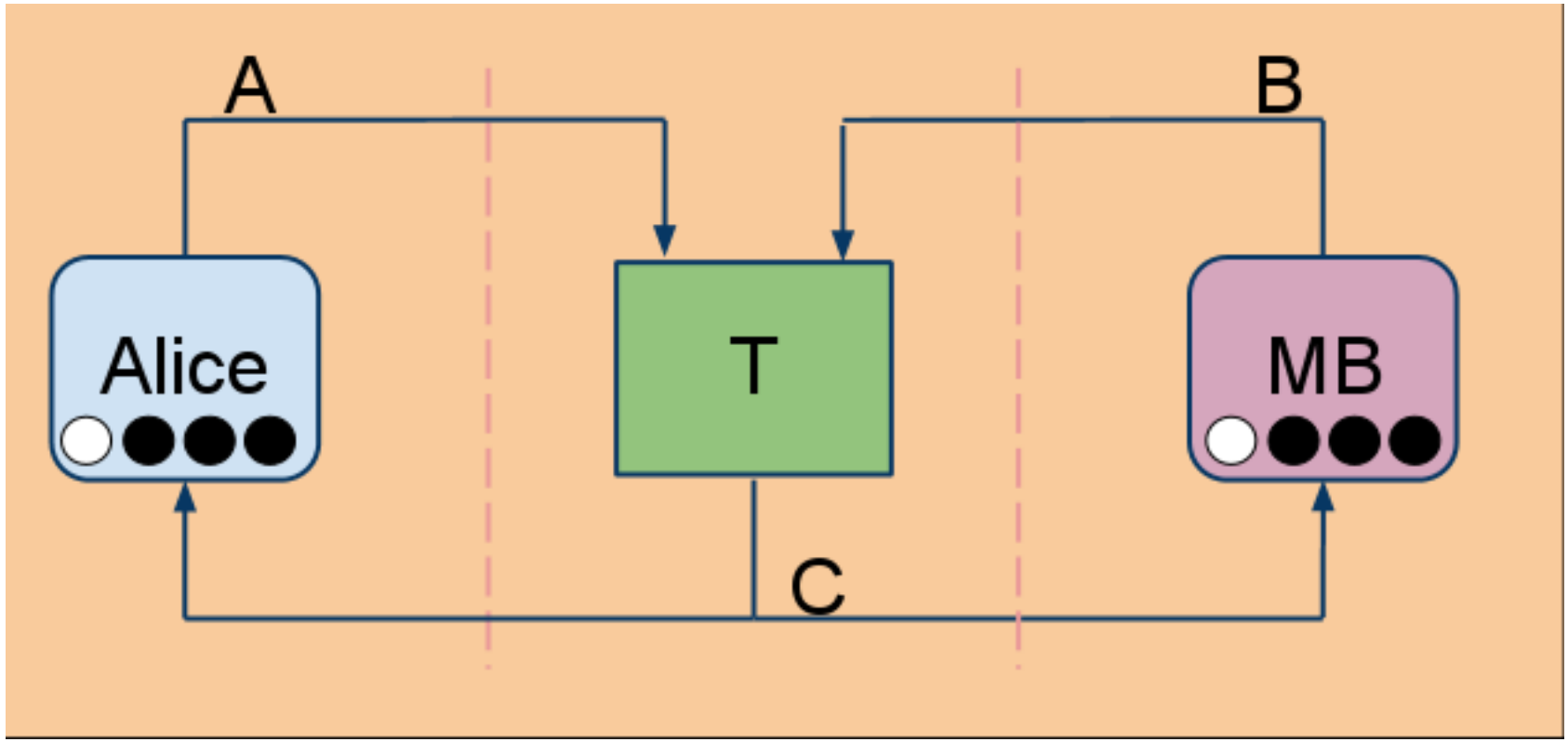
- Alice sends a 4-bit sequence to MB "1 1 0 0"
- MB inserts error in bits 2 and 3

Our solution: detect a relay attack



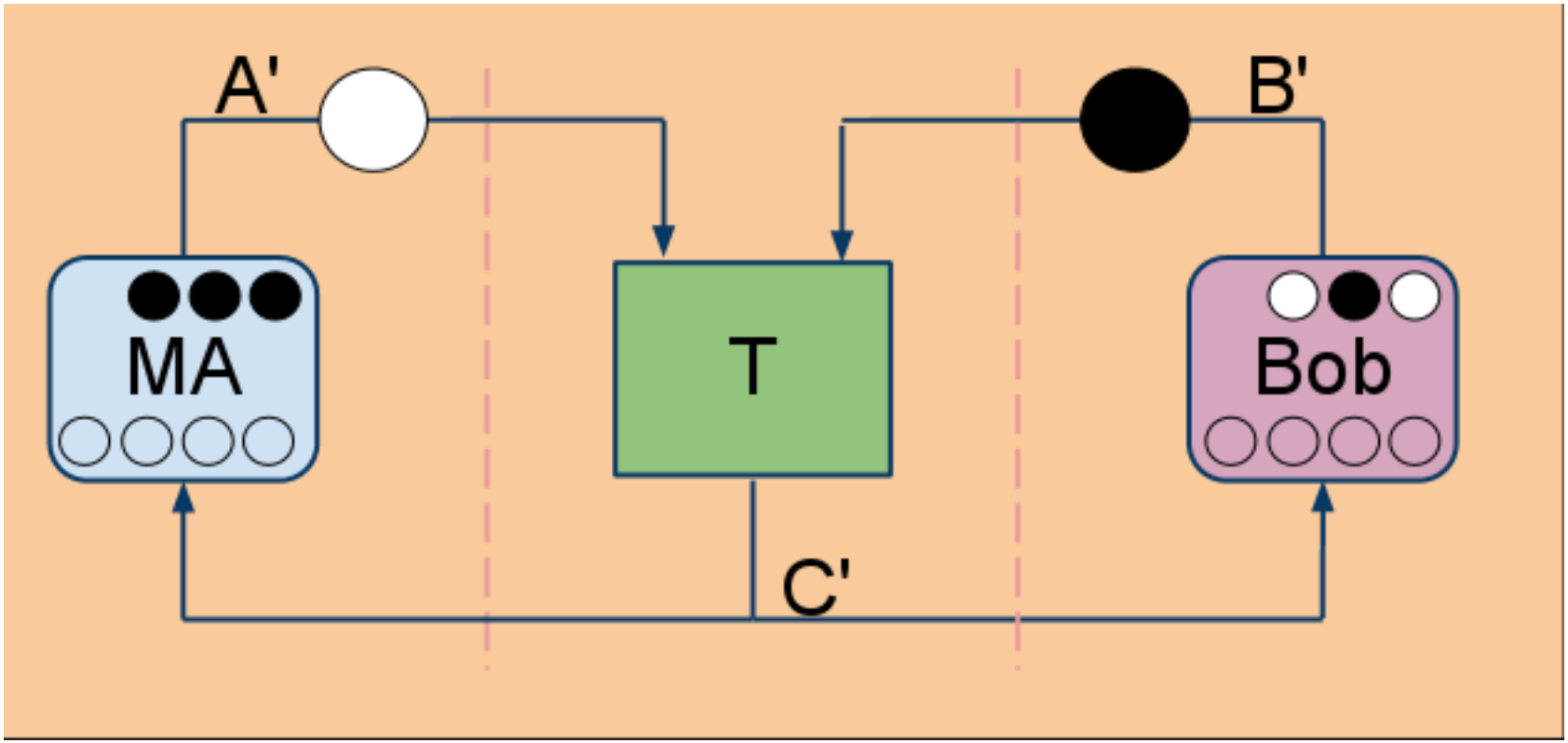
- Alice sends a 4-bit sequence to MB "1 1 0 0"
- MB inserts error in bits 2 and 3

Our solution: detect a relay attack



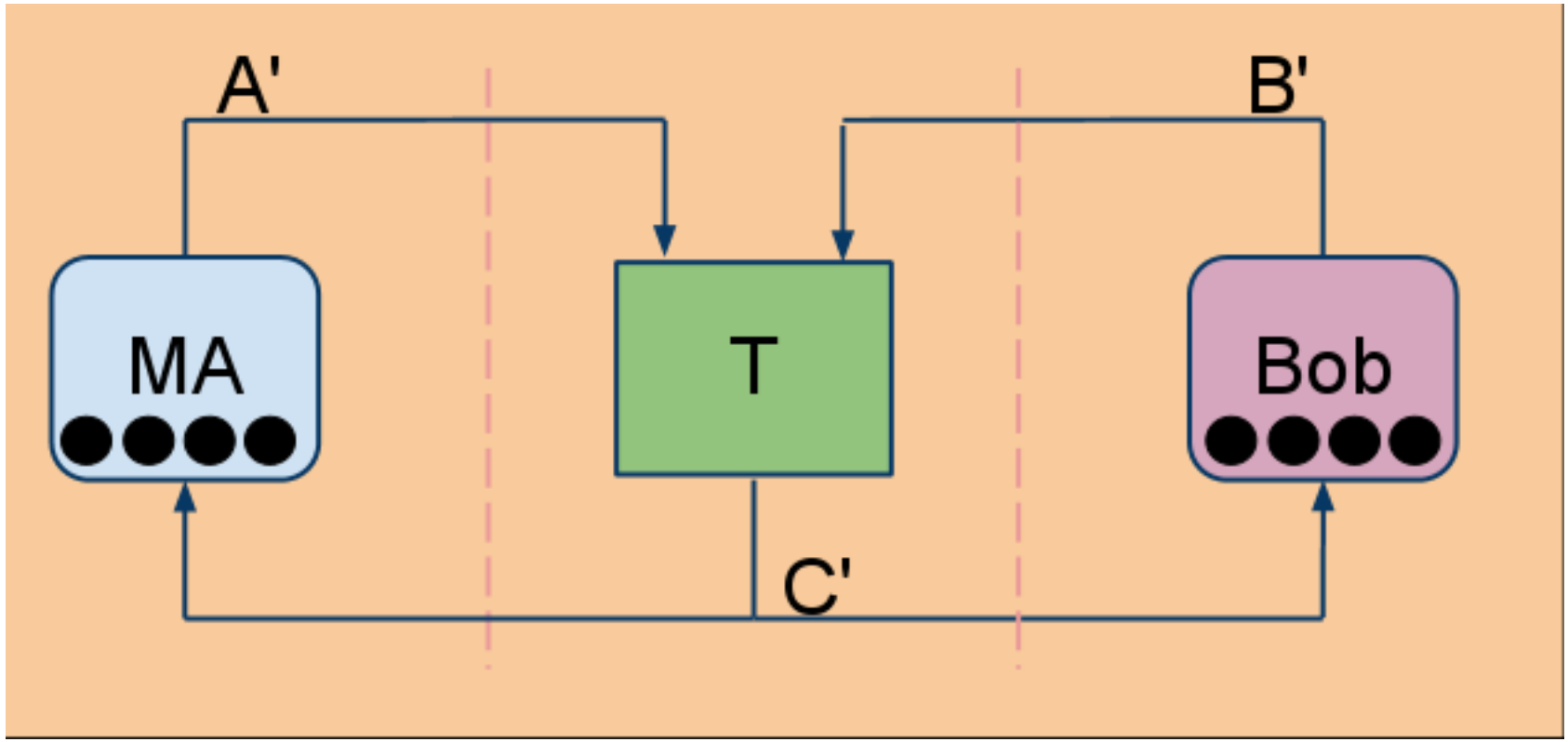
- Alice expects from Bob 3 out of 4 bits correct, i.e. sequence "1 0 0 0"
- MB inserts relays this to MA

Our solution: detect a relay attack



- MA forwards the data to Bob
- Bob introduces errors at bits 1 and 3

Our solution: detect a relay attack



- Bob receives "0 0 0 0" and sends this to Alice using encryption
- Alice spots the difference between this and the expected "1 0 0 0" => end of transaction

Limitations

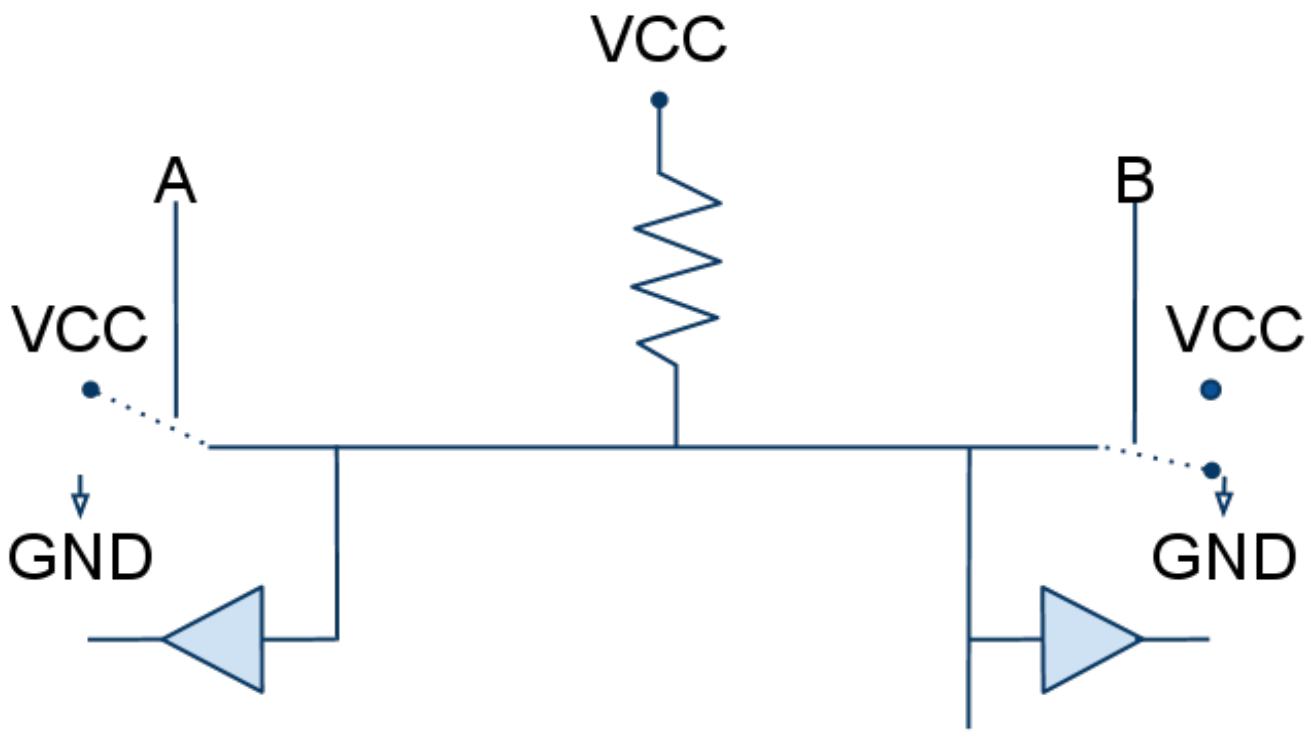
- No protection against long-cable relay attack
- In the example implementations, the attackers can read/write bits faster than Alice/Bob if they have better hardware => capability race

Questions

Presenter:

Omar Choudary (osc22@cam.ac.uk)
http://www.cl.cam.ac.uk/~osc22/

Implementation - example 2



- Bidirectional channel, e.g. ISO 7816
- Alice and Bob can send 0 (GND), 1 (VCC), or listen (state Z, pull-up resistor)

Implementation - example 2

- Protocol:
  - A, B: R_K (random based on secret)
  - For i=1,N
    - Alice sends either R_K[i] or listens
    - Bob does the same
  - They should only listen simultaneously for 25% of the bits
  - if a pair of attackers were involved this should be detected by
    - causing a short-circuit (bad sequence)
    - listening too much