Some Odd Problems in Crypto

Viet Tung Hoang

Agenda

1. The dating problem

2. Telephone coin flipping

The Dating Problem

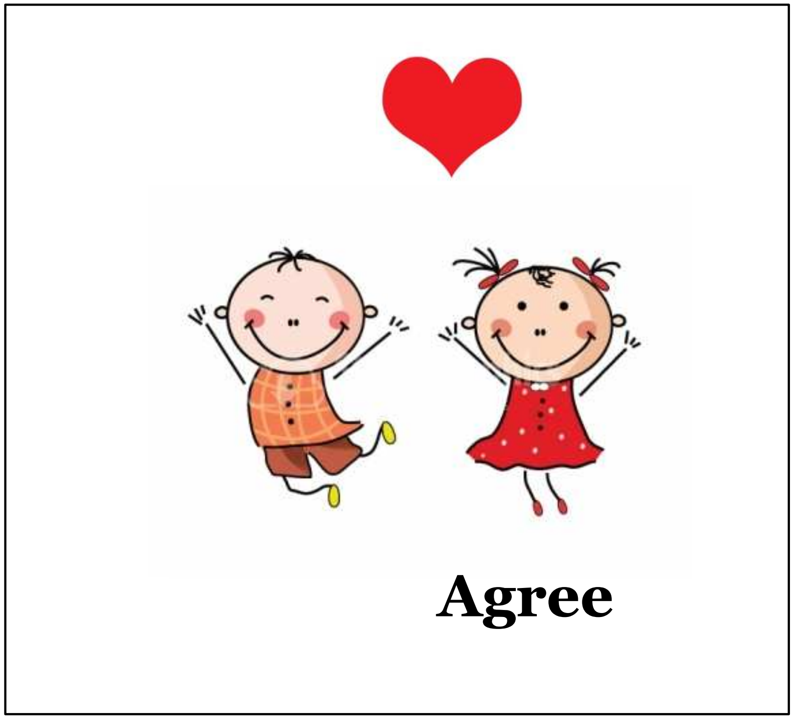
Issue: Embarrassing if one wants a second date while the other doesn't.

Privacy for The Dating Problem

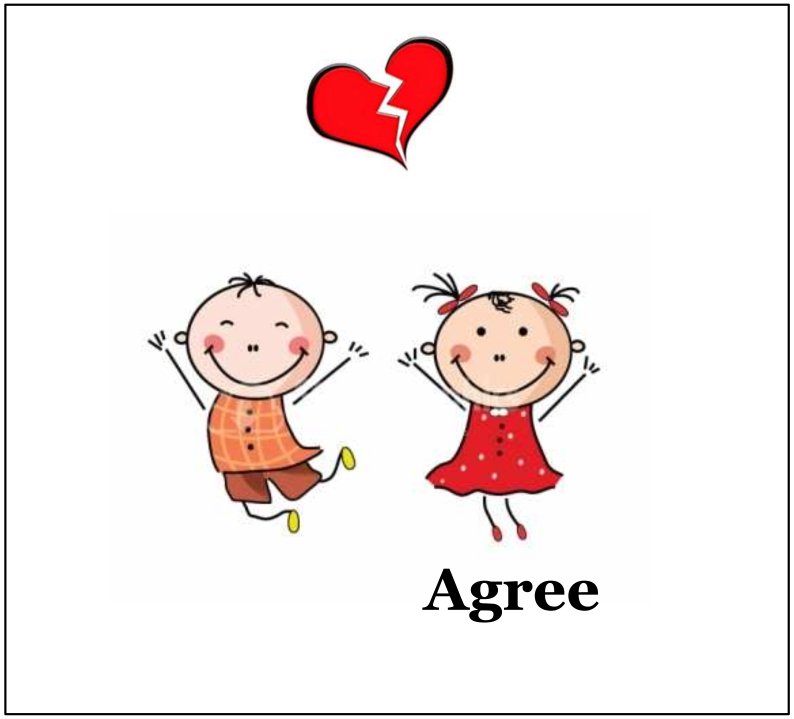
Want: Each person only knows:

- His/her choice & the final outcome
- Whatever **can be inferred** from the above

Bob's Privacy for the Dating Problem



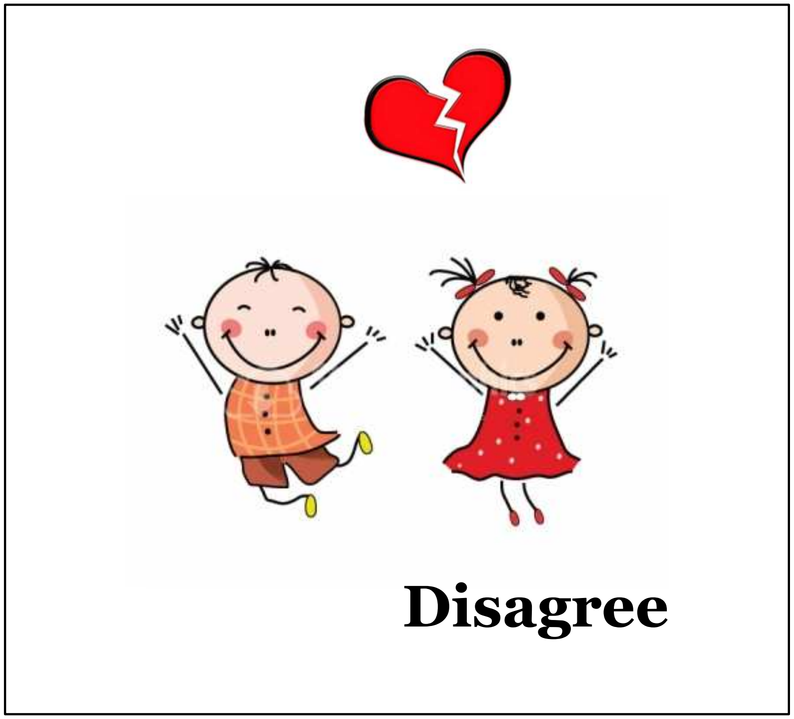
Alice knows Bob's input = "agree"



Alice knows Bob's input = "disagree"

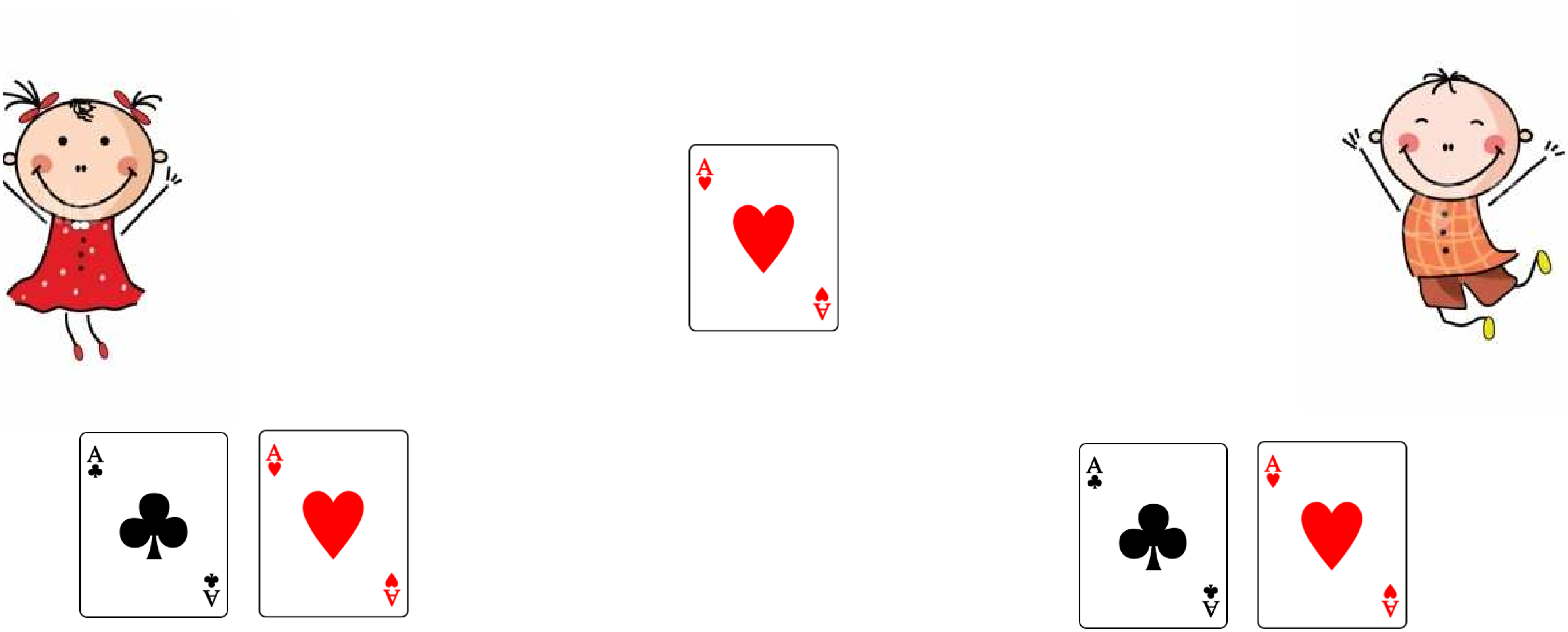
In those cases Bob's privacy is moot

Bob's Privacy for the Dating Problem

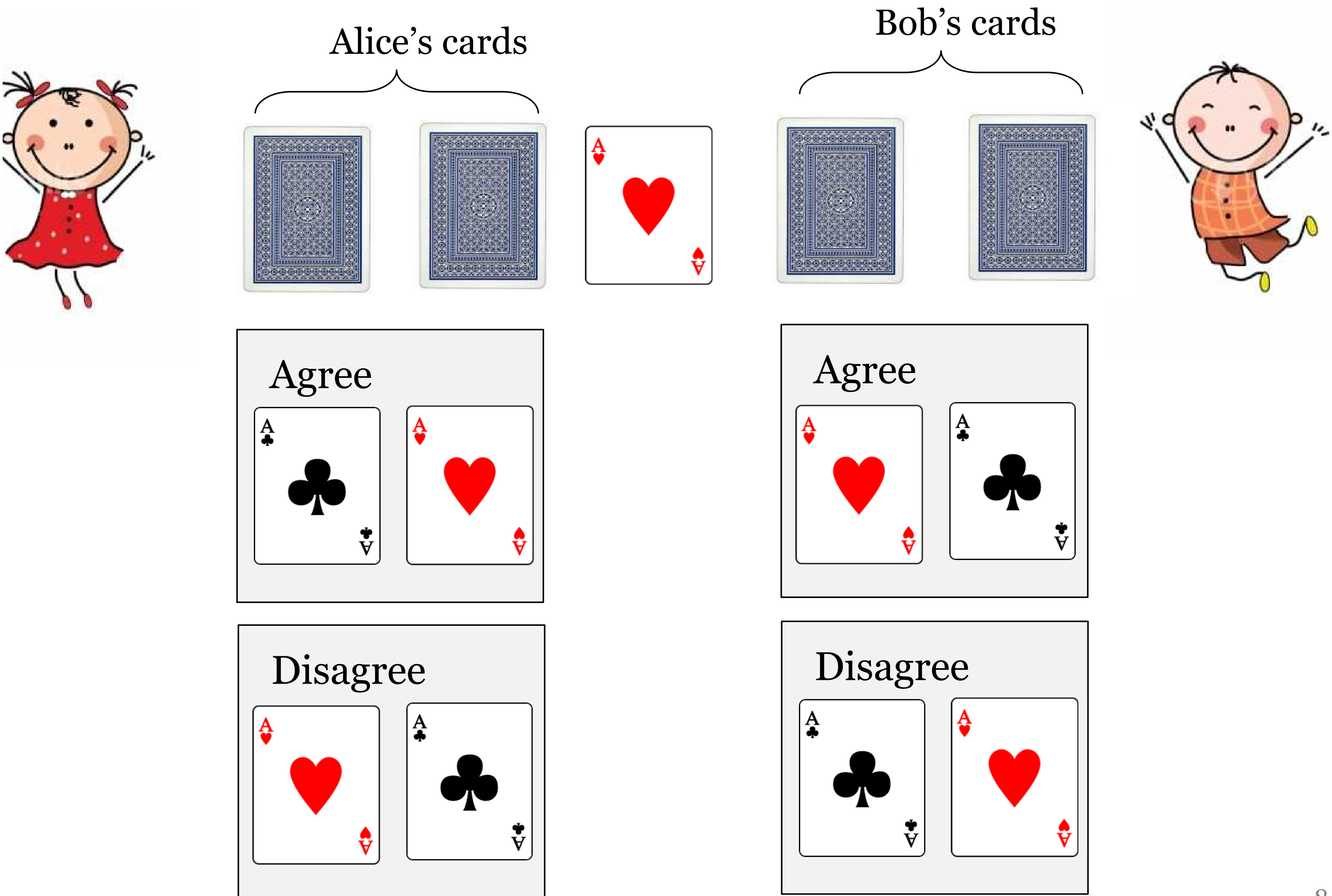


Must reveal **no information** about Bob's input

How to Solve the Dating Problem: 5-card Trick



How to Solve the Dating Problem: 5-card Trick



How to Solve the Dating Problem: 5-card Trick

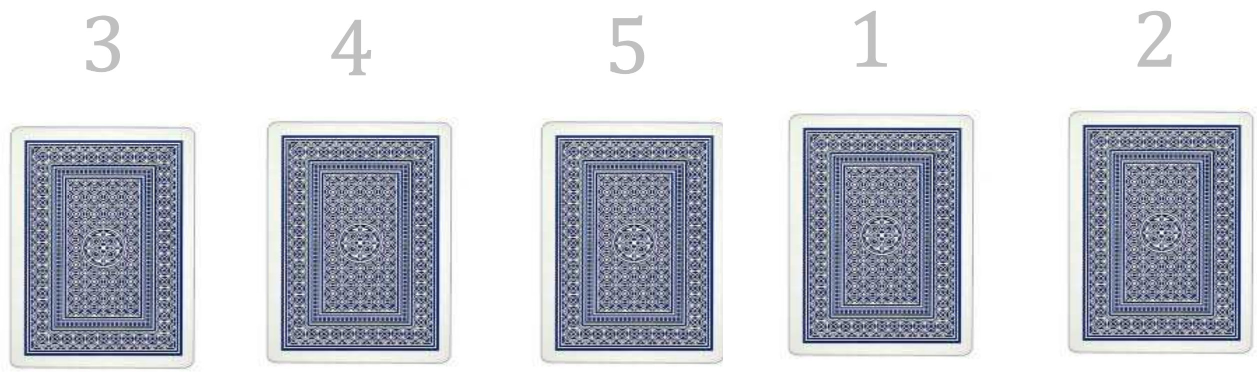
1 2 3 4 5

Alice's cut

Each takes turn to make a **private** cut

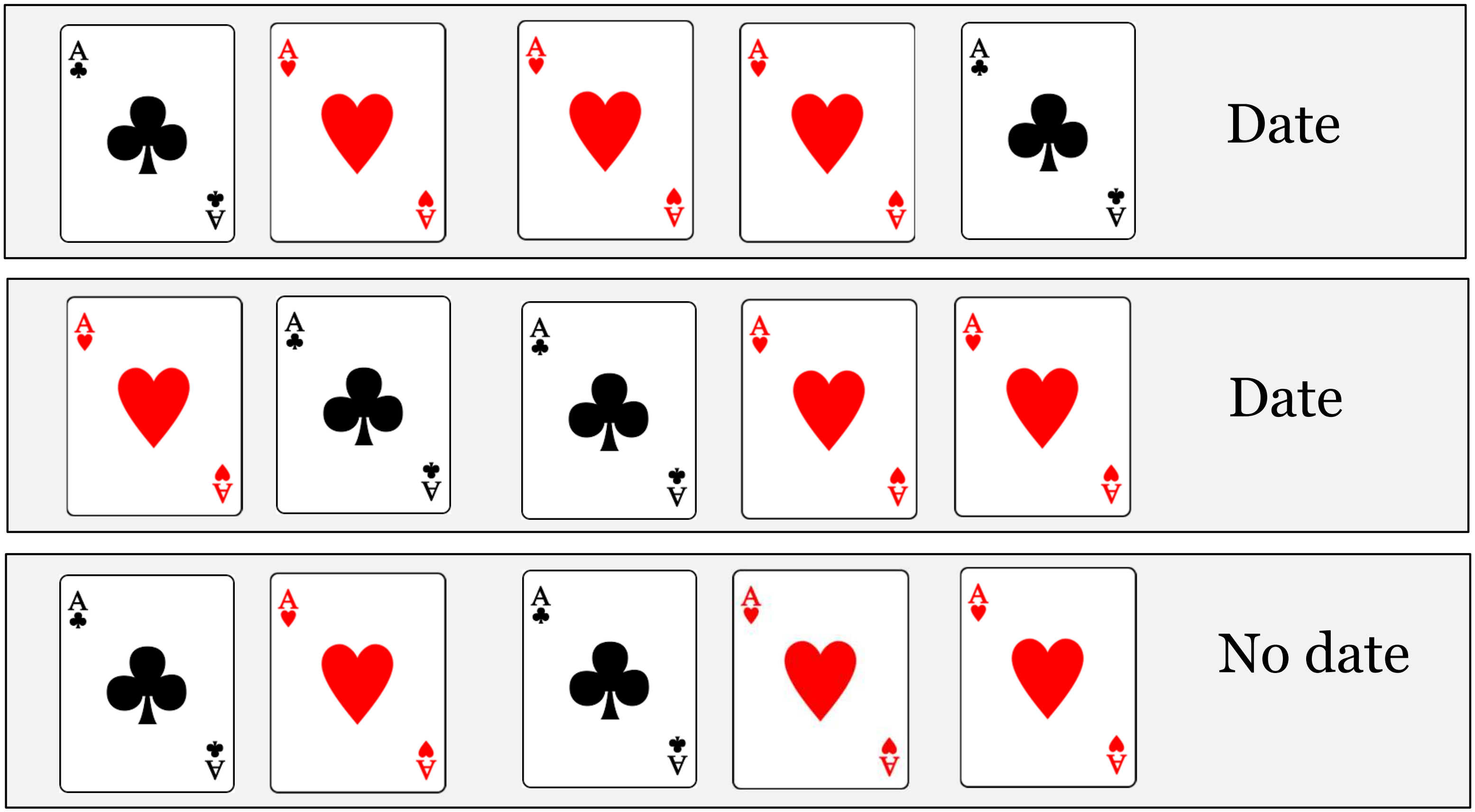
How to Solve the Dating Problem: 5-card Trick

Bob’s cut



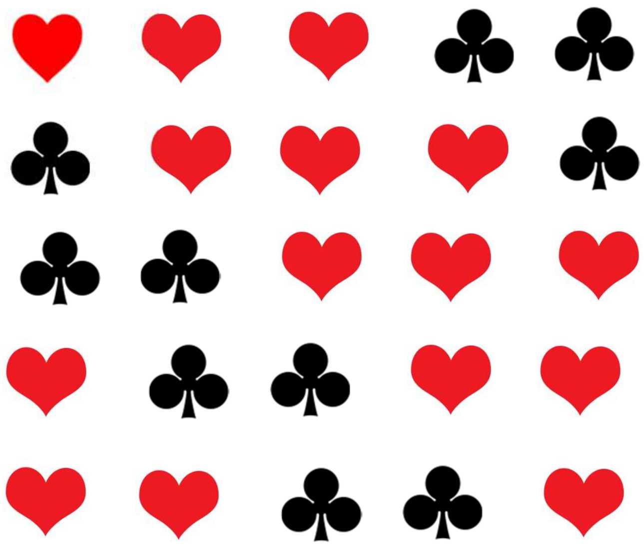
Each takes turn to make a **private** cut

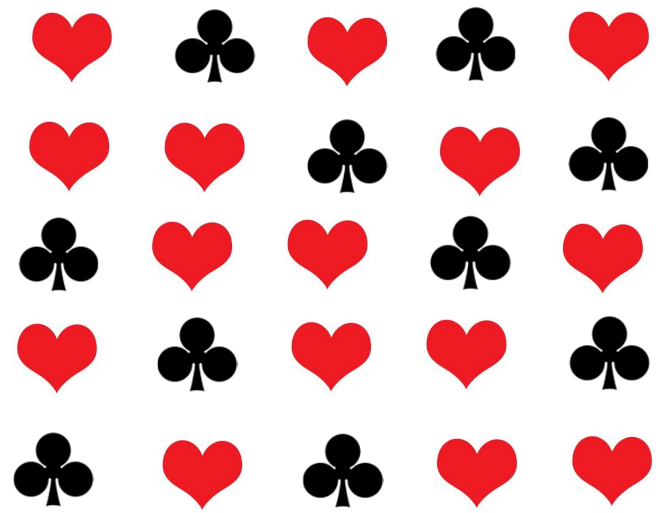
How to Solve the Dating Problem: 5-card Trick



If three ♥ in a (wrap-around) row then date. Otherwise no date

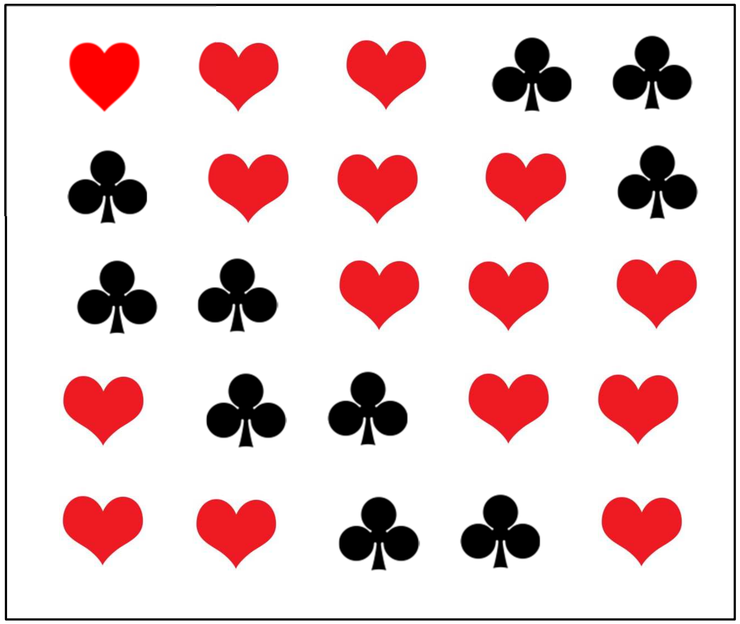
Why Is the Solution Correct?

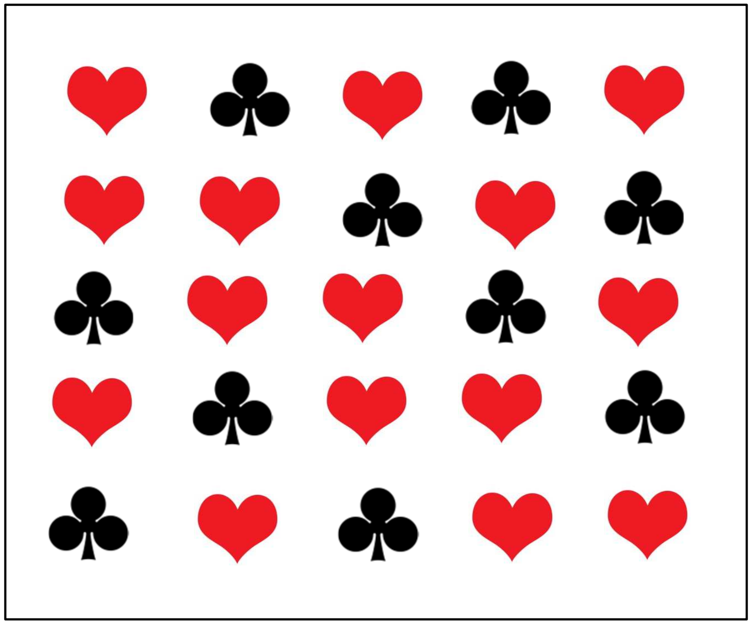


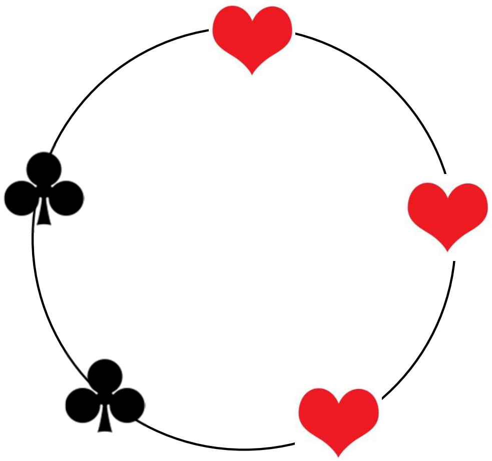


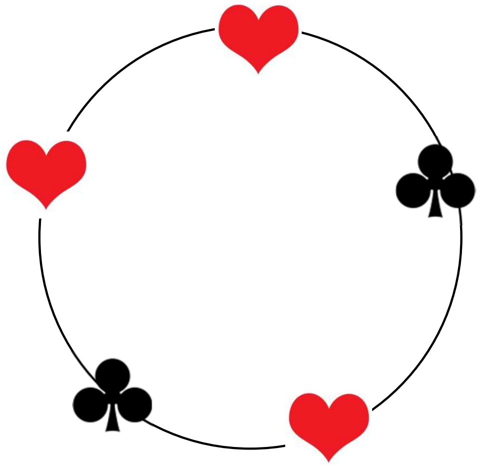
There are **ten** ways to place 3 ♥ and 2 ♣ in a line

But There Are Two Groups When Wrap Around

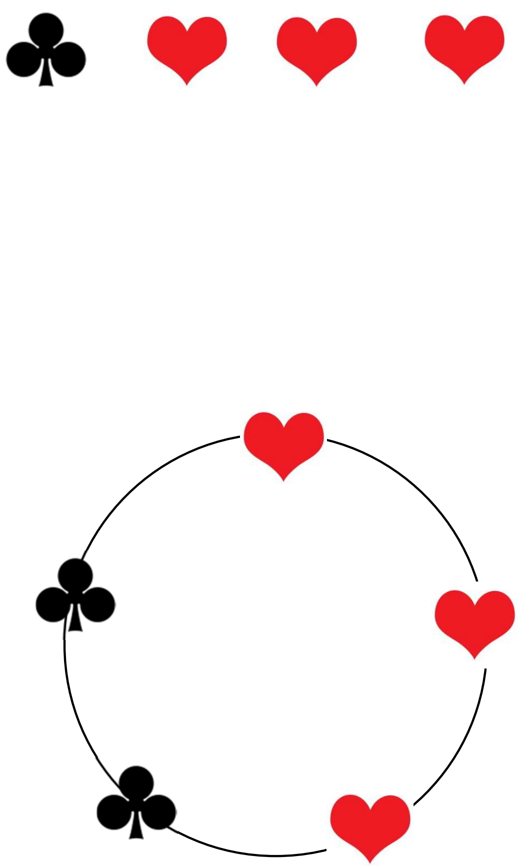




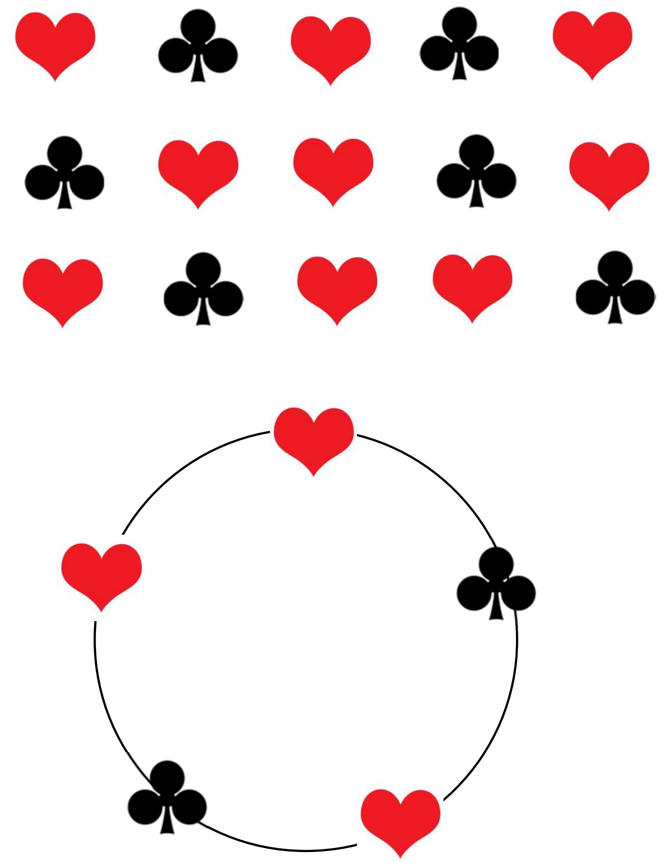




The Initial Place



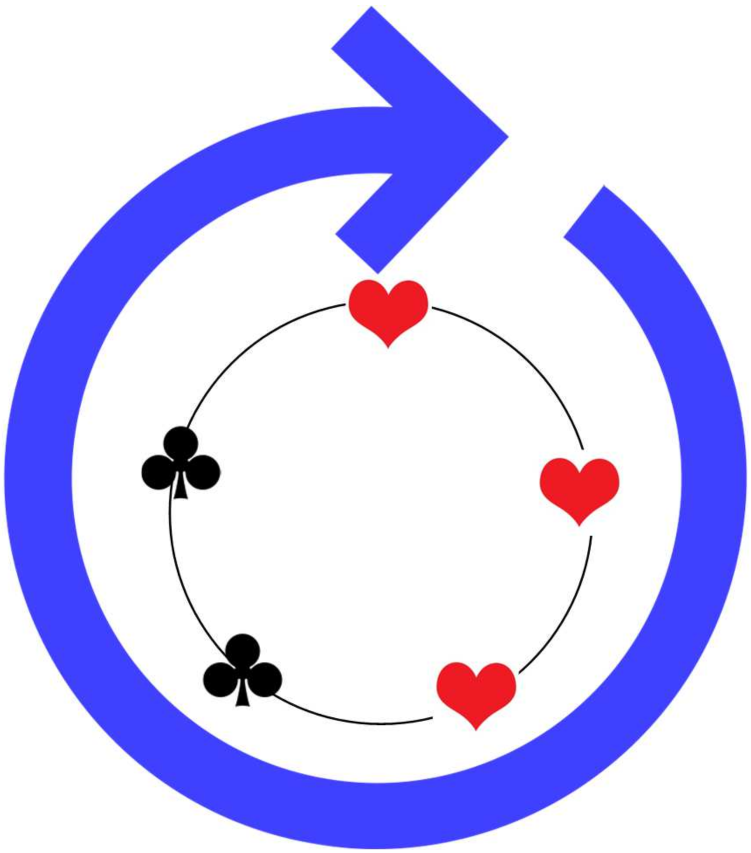
Date: Group 1

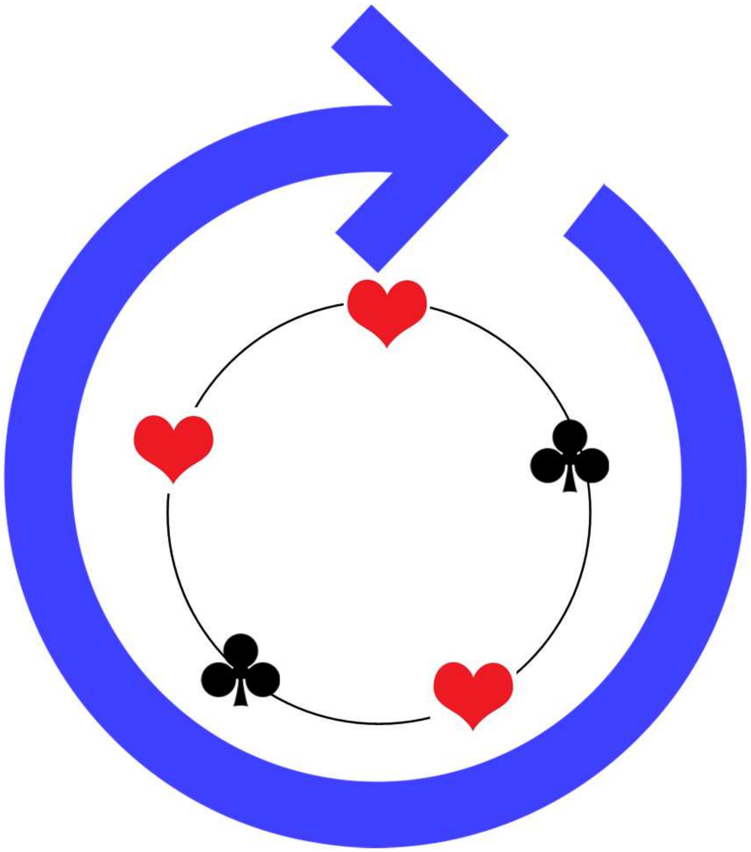


No Date: Group 2

Cutting Doesn't Change the Group

Circular shift





Why Is the Solution Private?

Your Exercise

Agenda

1. The dating problem

2. Telephone coin flipping

Telephone Coin Flipping


Alice and Bob wan to decide who gets the car (**over the phone**)

Alice's proposal:

•Alice tosses a coin and **informs** Bob of the outcome

•Bob gets the car if the coin lands head

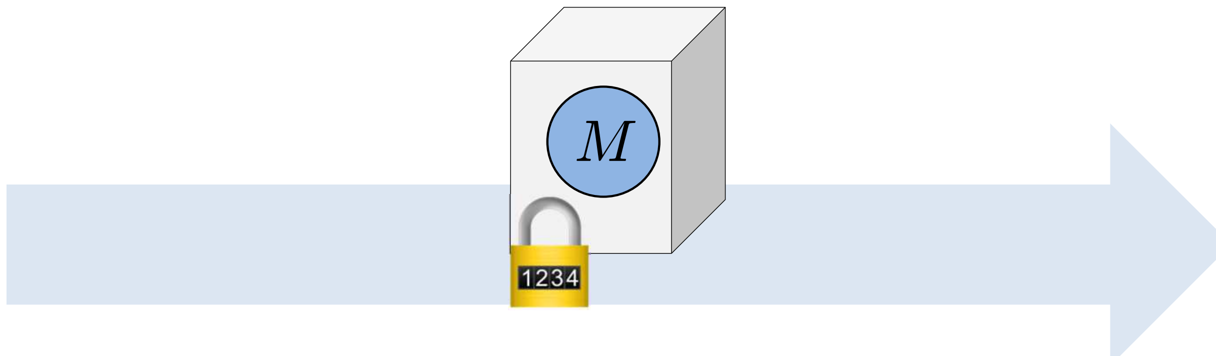
Telephone Coin Flipping

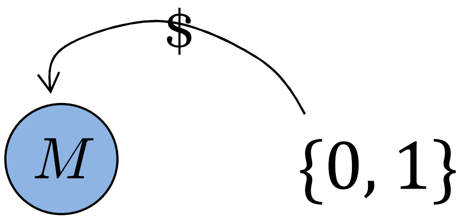

Goal:

-Both Alice and Bob learn the outcome of a fair coin toss

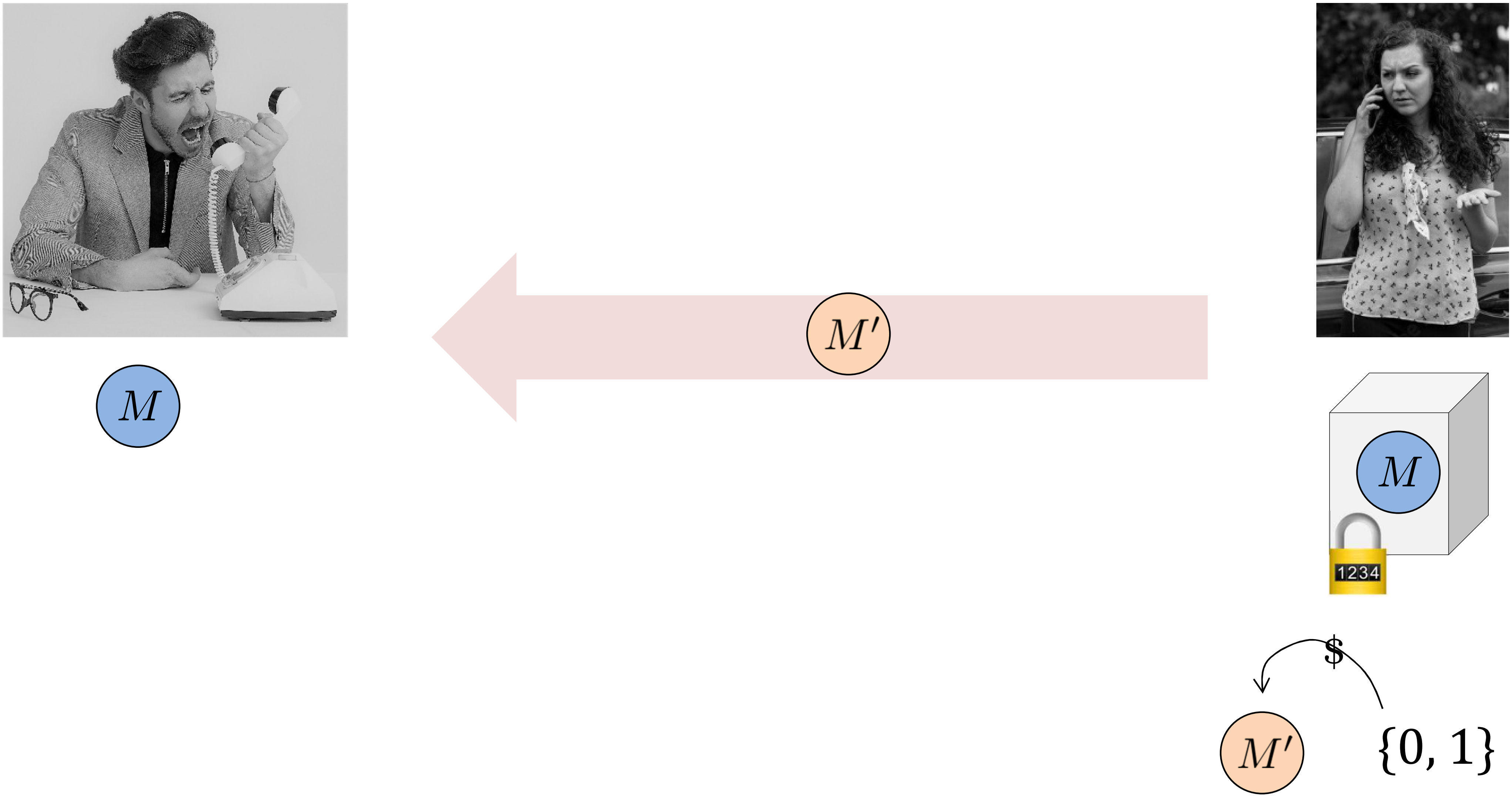
-Nobody can cheat the other

A Physical Solution

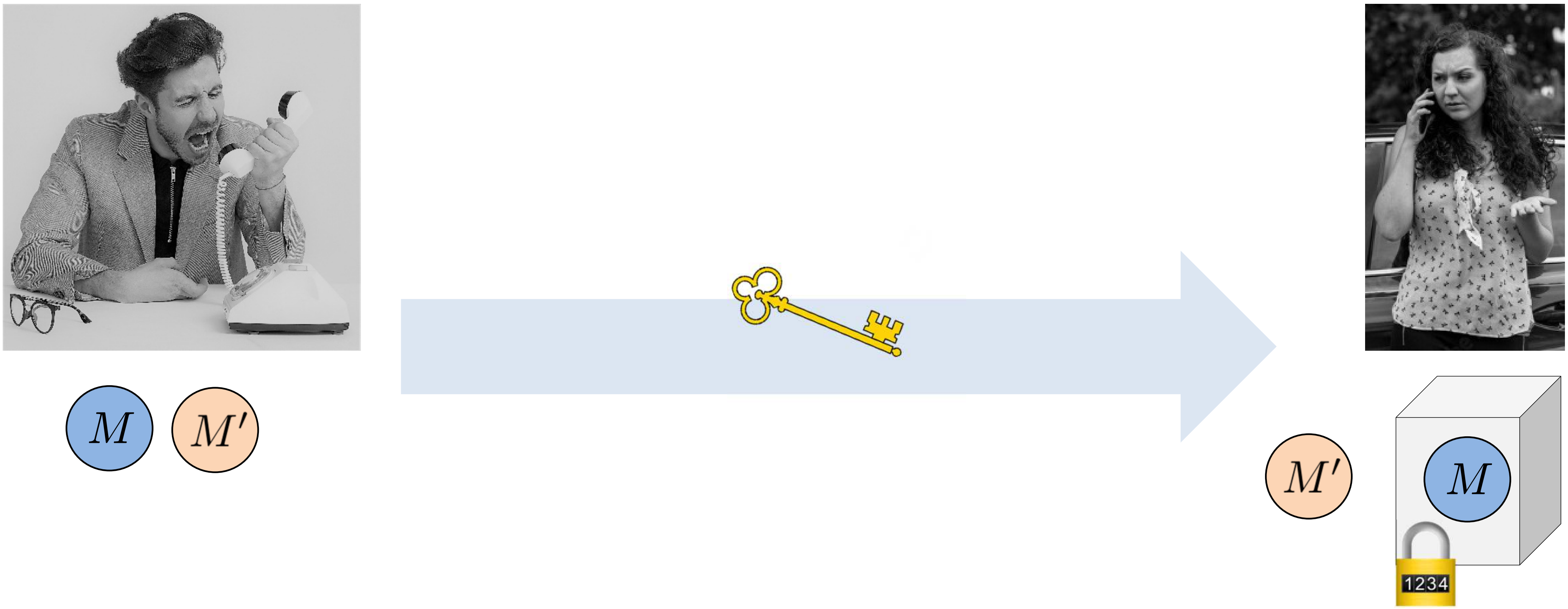




A Physical Solution



A Physical Solution



A Physical Solution

M M'

Output = $M \oplus M'$

M' M

How to Implement A Digital Locked Box

First attempt:

-A locked box containing a bit M is an encryption $C \leftarrow E_K(M)$

-The key to open the box is the key K

What can go wrong?

- Bob can send a **fake** key K' so that $E_{K'}^{-1}(C)$ is **another** bit of her choice

We Actually Need a Bit Commitment Scheme

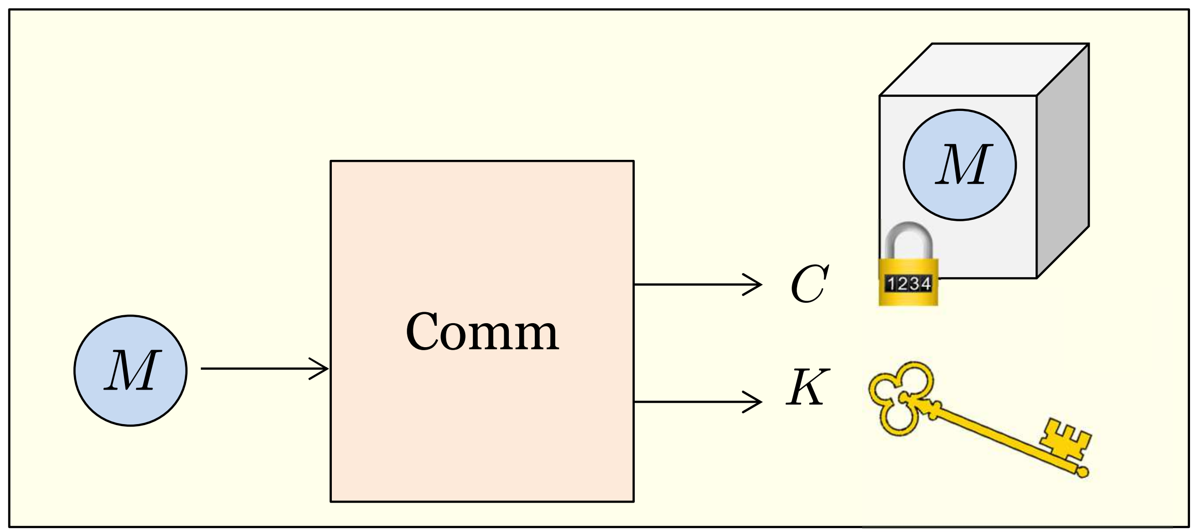
Commit: $(C, K) \leftarrow \mathrm{Comm}(M)$

$M \in \{0, 1\}$

Decommit: $M' \leftarrow \mathrm{DeComm}(K, C)$

$M' \in \{0, 1\} \cup \{\perp\}$

How to put a bit in a locked box



We Actually Need a Bit Commitment Scheme

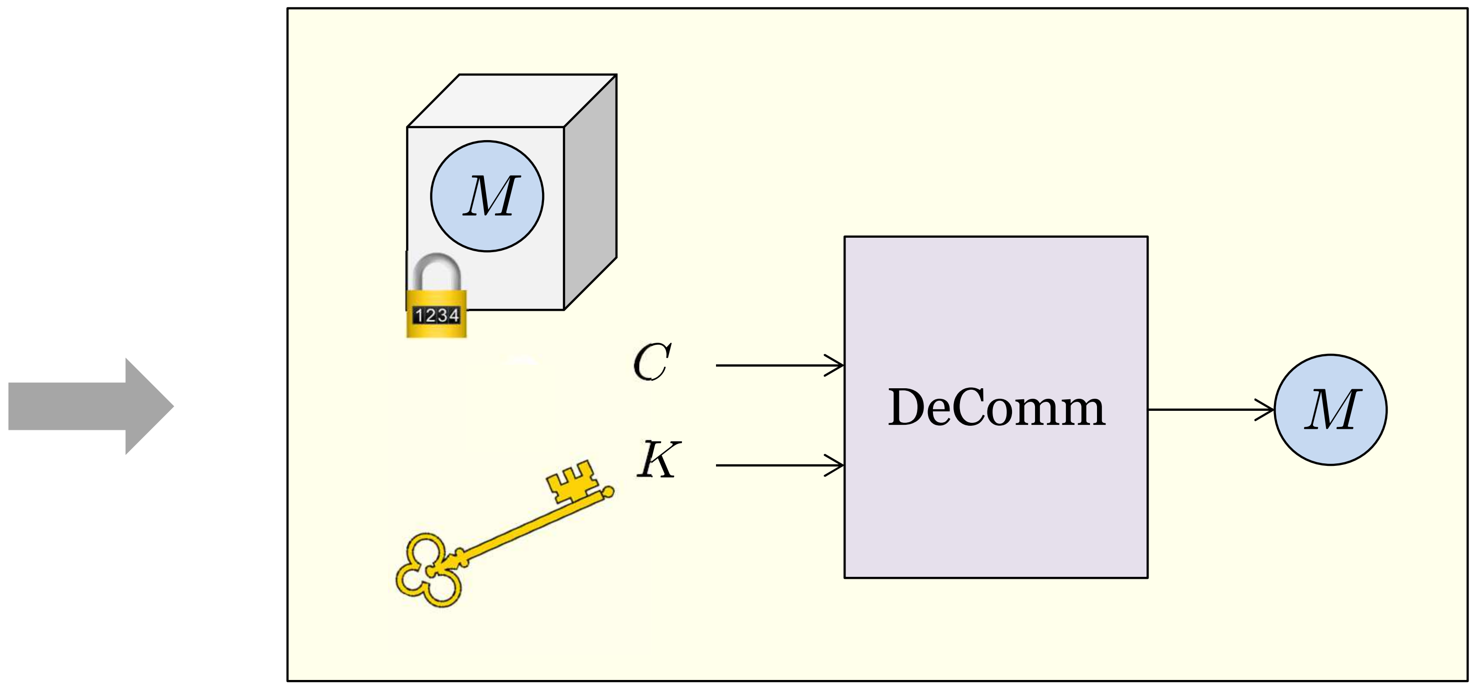
Commit: $(C, K) \leftarrow \mathrm{Comm}(M)$

$M \in \{0, 1\}$

Decommit: $M' \leftarrow \mathrm{DeComm}(K, C)$

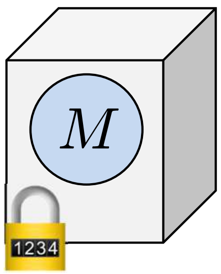
$M' \in \{0, 1\} \cup \{\perp\}$

How to open



Security Requirements of Bit Commitment

Hiding: Committal C reveals **nothing** about M

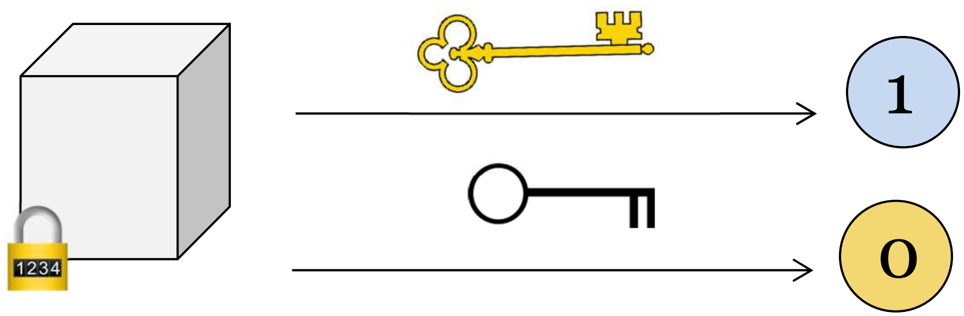


Alice can't learn the value in the locked box

Security Requirements of Bit Commitment

Binding: It's **hard** to find C^*, K_0, K_1 such that

$$\mathrm{DeComm}(K_0, C^*) = 0 \text{ and } \mathrm{DeComm}(K_1, C^*) = 1$$



Bob can't construct a box that he can open to both 0 and 1

A Simple Bit Commitment Scheme

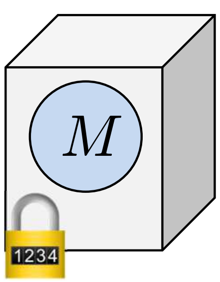
Commit to 0:

- Pick two 1024-bit primes p, q such that $\begin{cases} p < q \\ p \equiv 3 \pmod 4, \; q \equiv 1 \pmod 4 \end{cases}$

Commit to 1:

- Pick two 1024-bit primes p, q such that $\begin{cases} p < q \\ p \equiv 1 \pmod 4, \; q \equiv 3 \pmod 4 \end{cases}$

Commital: $N = pq$



Key: (p, q)

Implementing Decommitment

Try this at home