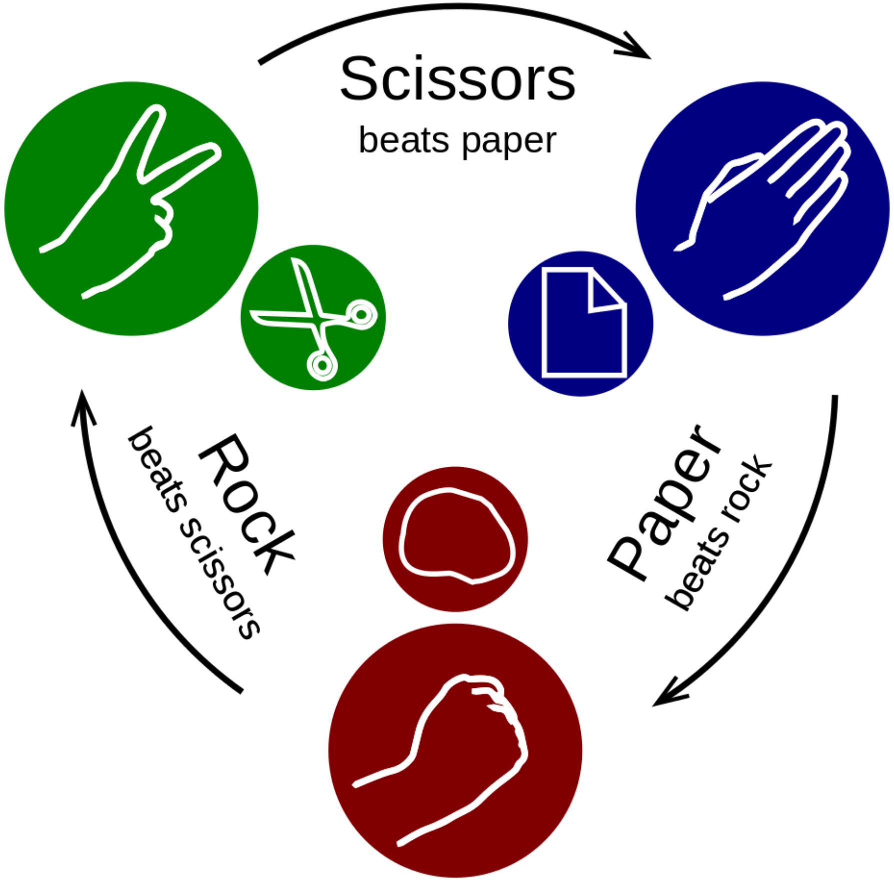
UNIVERSITY OF TWENTE.

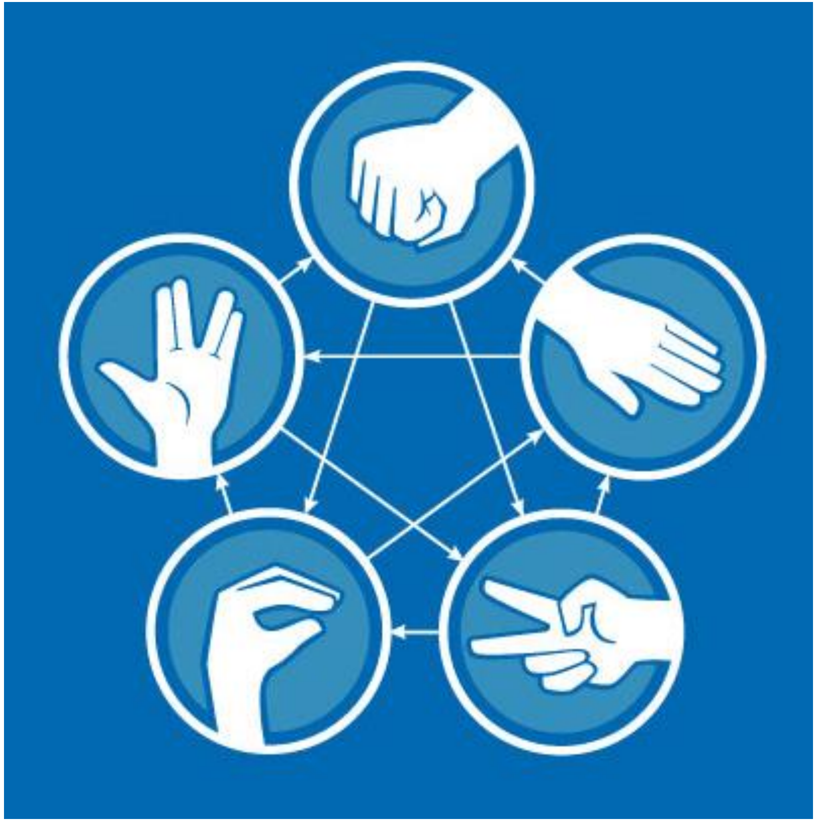
Commitments

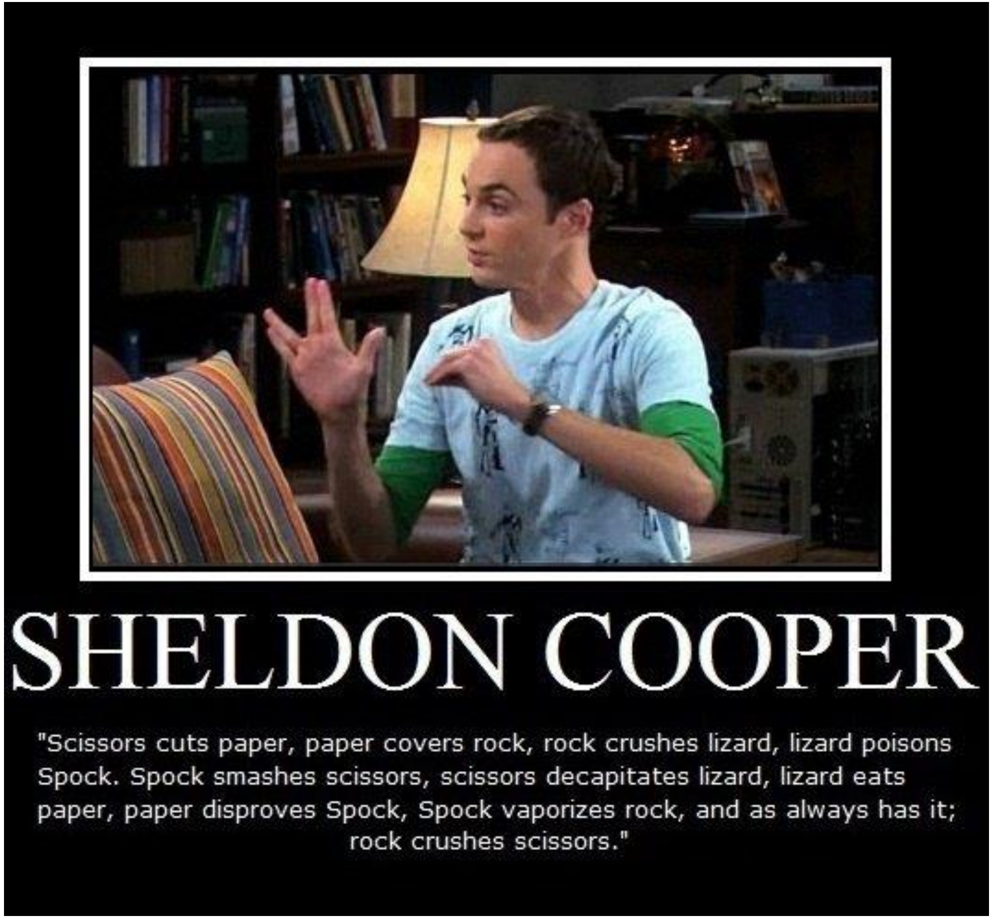
Topic of Software Systems (TCS module 2)

Lecturer: Maarten Everts



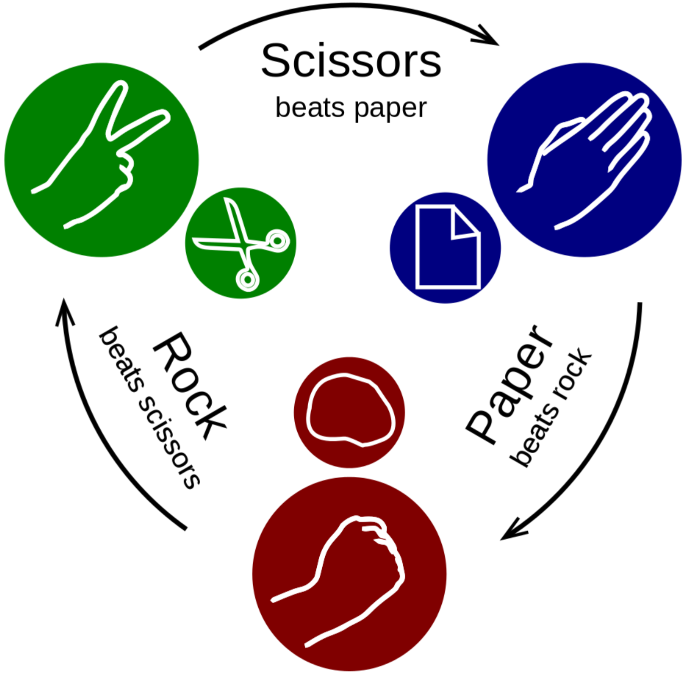
UNIVERSITY OF TWENTE.





SHELDON COOPER

"Scissors cuts paper, paper covers rock, rock crushes lizard, lizard poisons Spock. Spock smashes scissors, scissors decapitates lizard, lizard eats paper, paper disproves Spock, Spock vaporizes rock, and as always has it; rock crushes scissors."

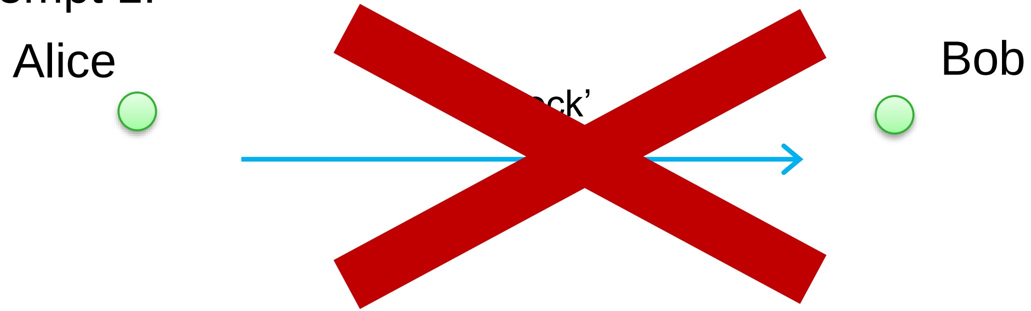


How to play rock-paper-scissors over the phone?

UNIVERSITY OF TWENTE.

Let’s try

Attempt 1:

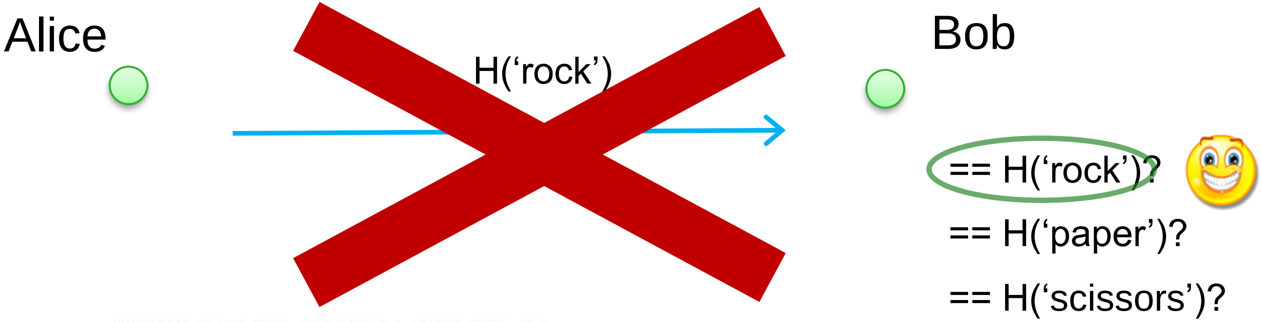


Alice

ck’

Bob

Attempt 2:



Alice

H(‘rock’)

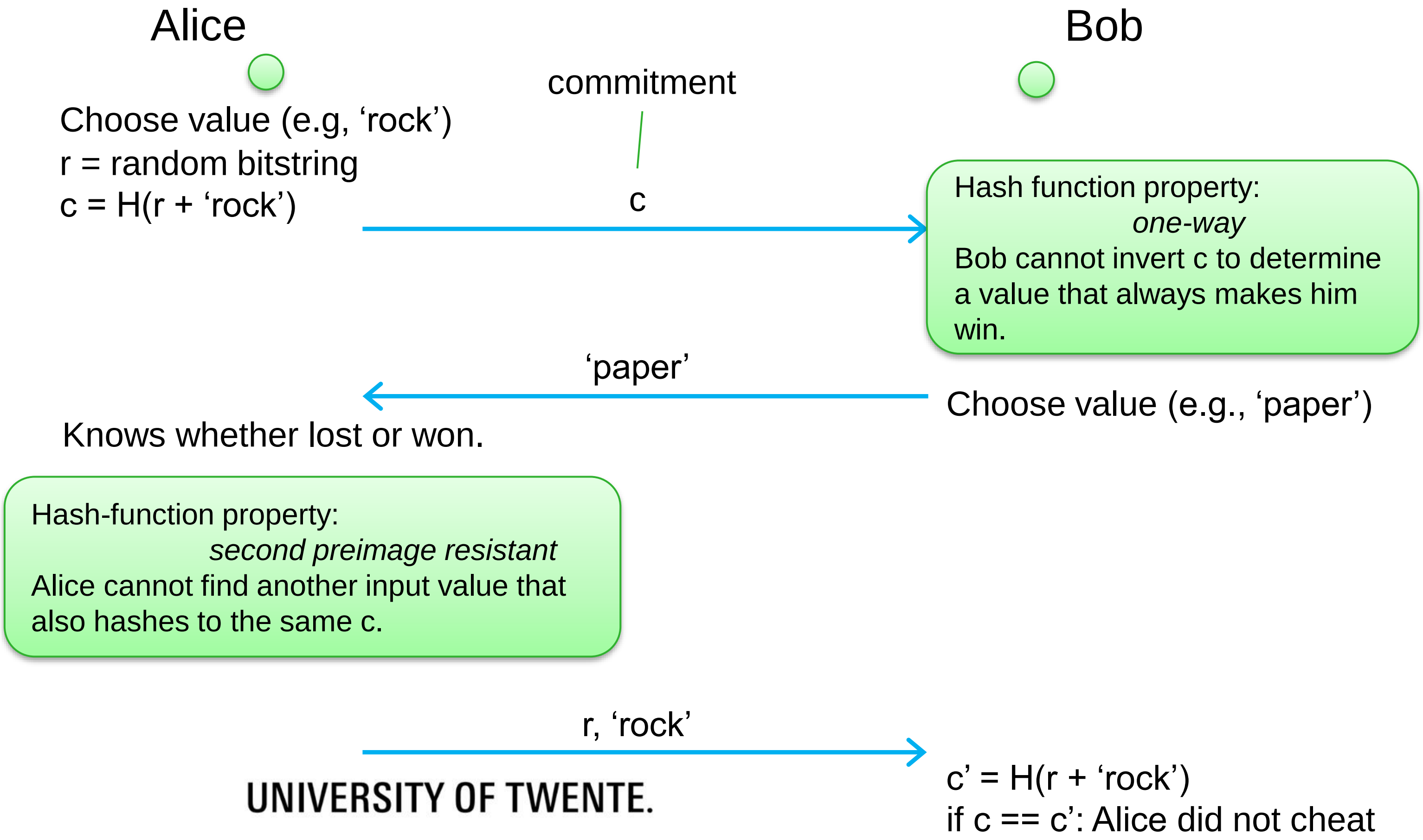
Bob

== H(‘rock’)?

== H(‘paper’)?

== H(‘scissors’)?

For example: `83751e164d08f068c33ca43d2cf0d9198b2432d4`



Alice

Bob

Choose value (e.g, ‘rock’)
r = random bitstring
c = H(r + ‘rock’)

commitment

c

Hash function property:
one-way
Bob cannot invert c to determine a value that always makes him win.

‘paper’

Choose value (e.g., ‘paper’)

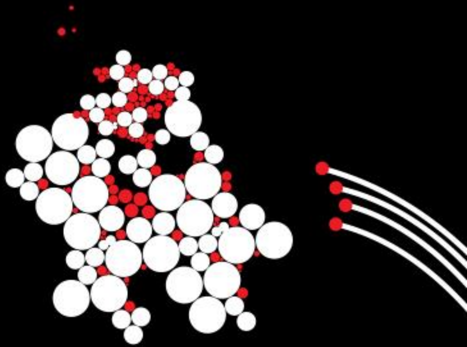
Knows whether lost or won.

Hash-function property:
second preimage resistant
Alice cannot find another input value that also hashes to the same c.

r, ‘rock’

c’ = H(r + ‘rock’)
if c == c’: Alice did not cheat

UNIVERSITY OF TWENTE.



Commitments

Topic of Software Systems (TCS module 2)

Lecturer: Maarten Everts