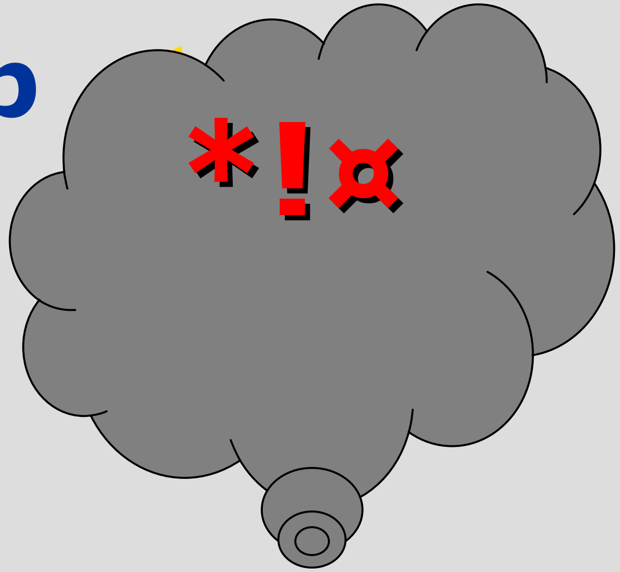
Quantum Bit Commitment

Christian Schaffner

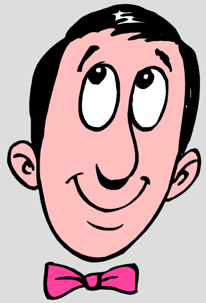
DAIMI – Department of Computer Science
BRICS – Basic Research in Computer Science

NAT-årsfest
June 3, 2005

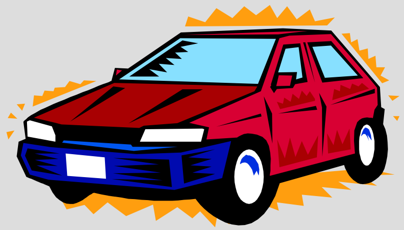
Alice & Bob



Alice



Bob

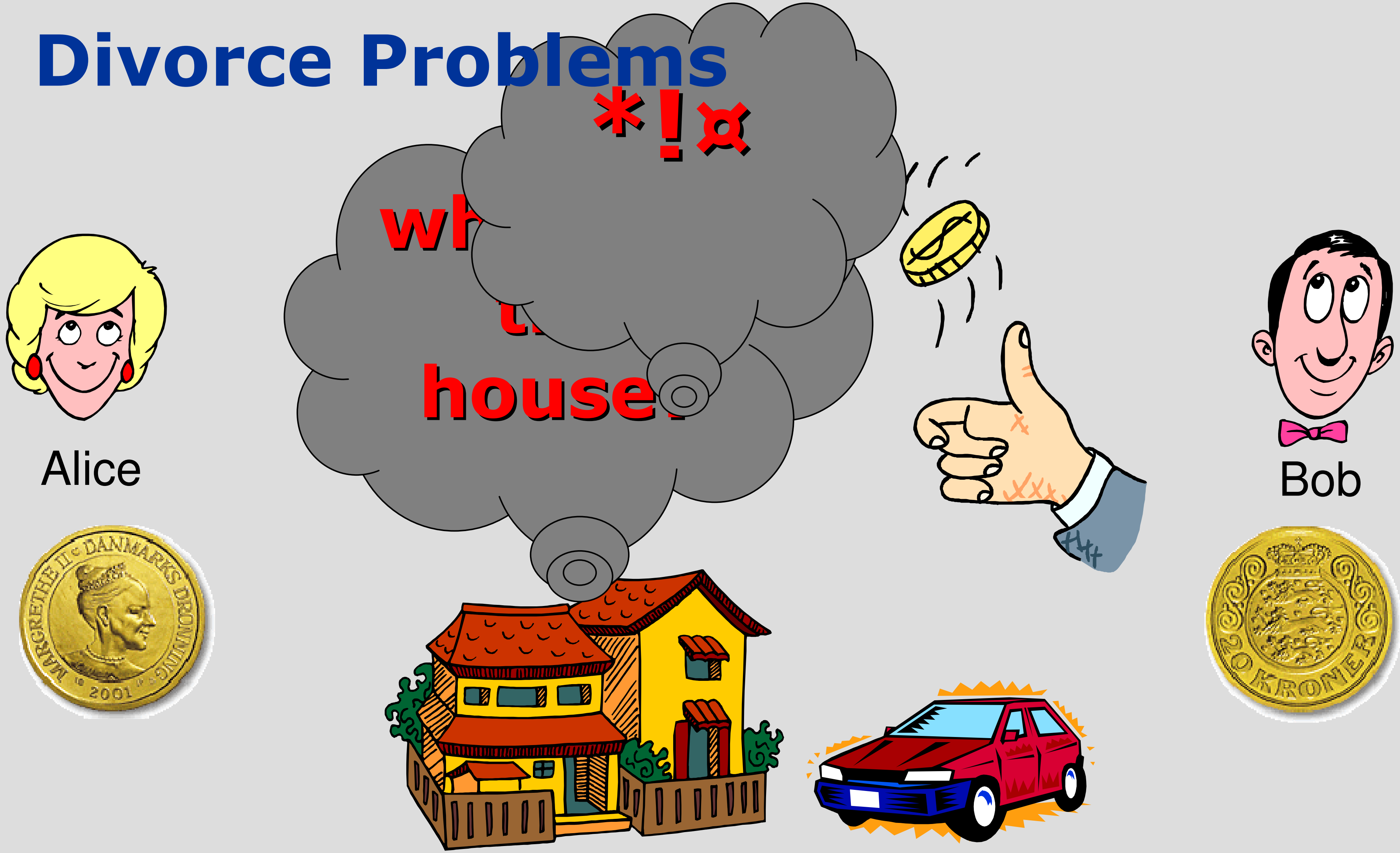


AARHUS UNIVERSITET

DAIMI – Department of Computer Science
BRICS – Basic Research in Computer Science

Christian Schaffner, PhD student
NF-årsfest 2005

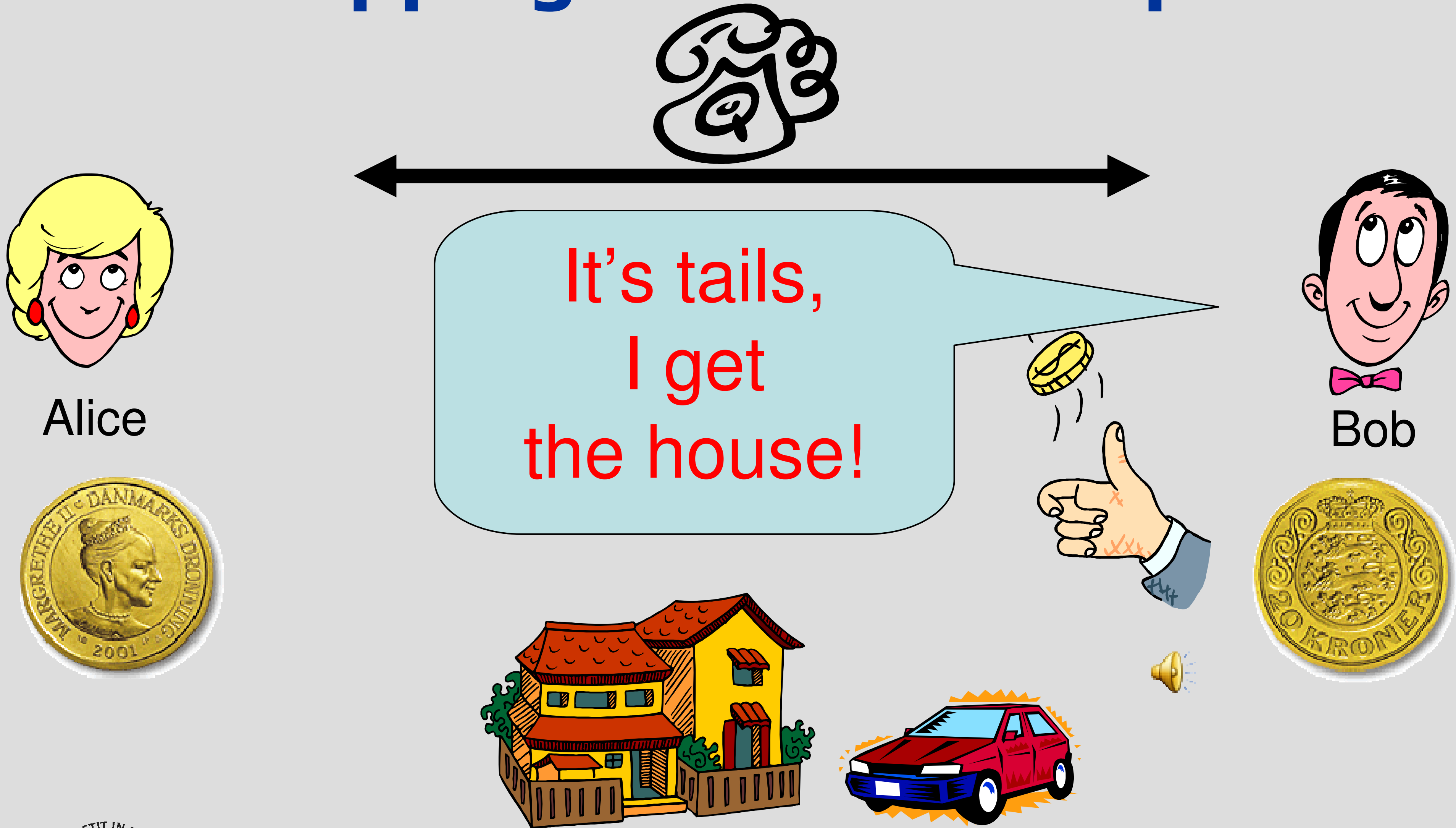
Divorce Problems



AARHUS UNIVERSITET
DAIMI – Department of Computer Science
BRICS – Basic Research in Computer Science

Christian Schaffner, PhD student
NF-årsfest 2005

Coin-Flipping over the Telephone



AARHUS UNIVERSITET

DAIMI – Department of Computer Science
BRICS – Basic Research in Computer Science

Christian Schaffner, PhD student
NF-årsfest 2005

A Coin-Flipping Protocol

$a \in_R \{0,1\}$ $\longrightarrow$

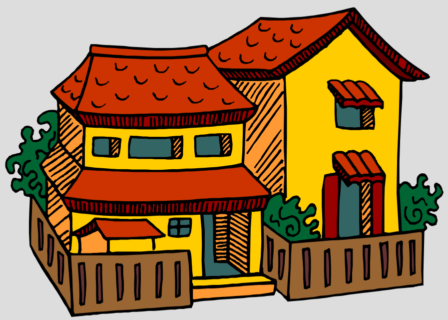
Alice

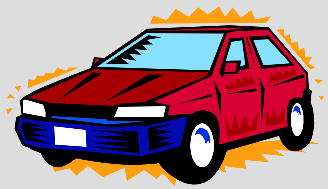
$b \in_R \{0,1\}$ $\longleftarrow$

not random!

Bob

$a = b$





$a \neq b$

SOLIDUM PETIT IN PROFUNDIS · UNIVERSITAS ARHUSIENSIS

AARHUS UNIVERSITET

DAIMI – Department of Computer Science
BRICS – Basic Research in Computer Science

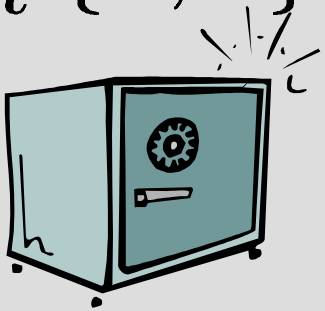
Christian Schaffner, PhD student
NF-årsfest 2005

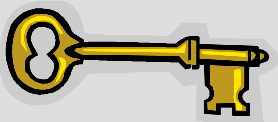
The Solution

$a \in_R \{0,1\}$

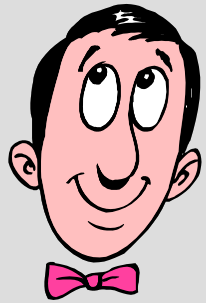
a

Alice



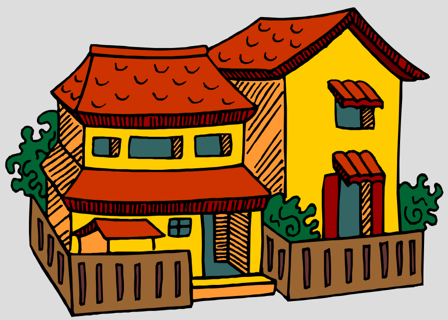


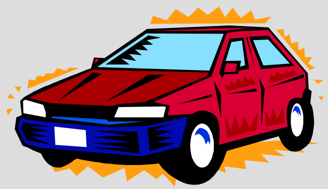
$b \in_R \{0,1\}$



Bob

$a = b$





$a \neq b$

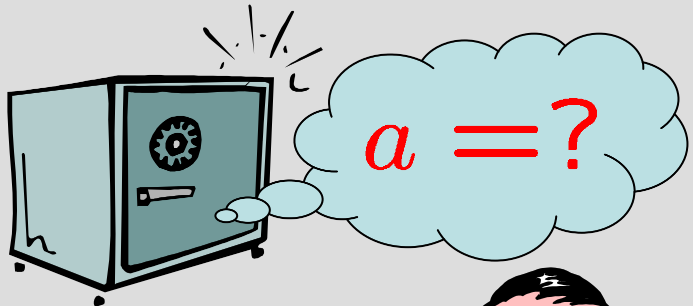
AARHUS UNIVERSITET

DAIMI – Department of Computer Science
BRICS – Basic Research in Computer Science

Christian Schaffner, PhD student
NF-årsfest 2005

The Explanation

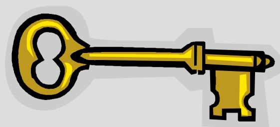
$a \in_R \{0,1\}$



Alice

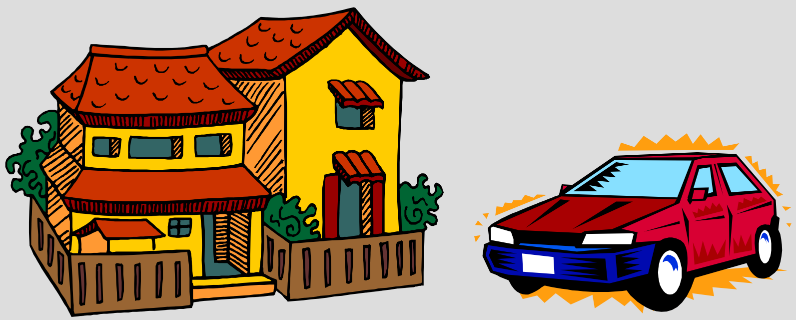
Bob

$b \in_R \{0,1\}$



a

$a = b$



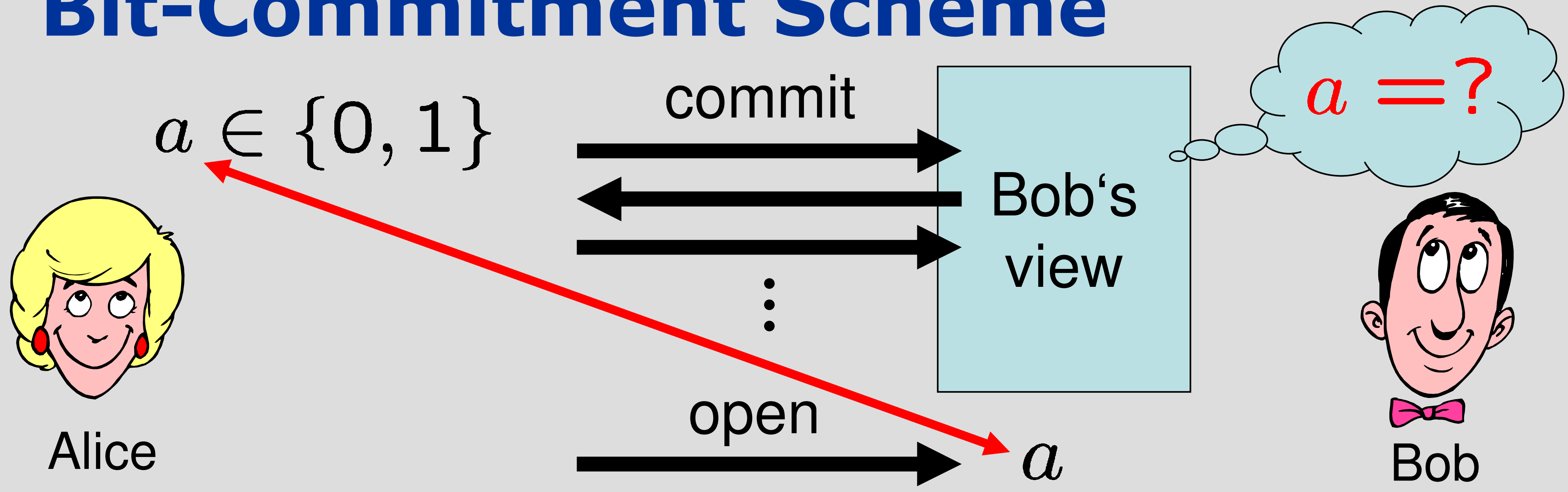
$a \neq b$

AARHUS UNIVERSITET

DAIMI – Department of Computer Science
BRICS – Basic Research in Computer Science

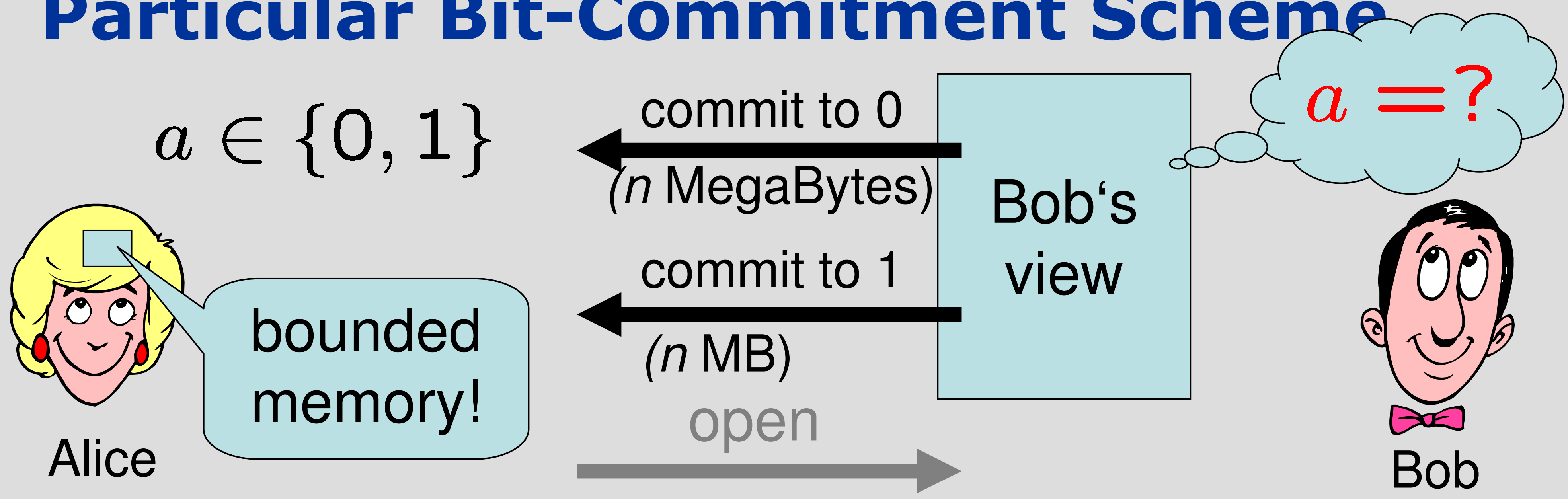
Christian Schaffner, PhD student
NF-årsfest 2005

Bit-Commitment Scheme



- important cryptographic primitive
- hiding
- binding

Particular Bit-Commitment Scheme



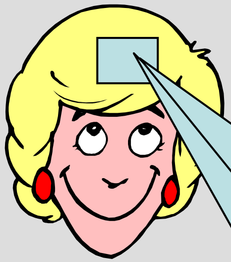
- honest Alice needs: n
- cheating Alice needs: $2 \cdot n$
- $\text{Memory}_{\text{cheater}} < 2 \cdot \text{Memory}_{\text{honest}} \Rightarrow$ binding
- perfectly hiding

Quantum Bit-Commitment Scheme

$a \in \{+, \times\}$

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

measure qbits in basis *a*



Alice

bounded memory!

memory!

n quantum bits

Bob's view

$a = ?$

Bob

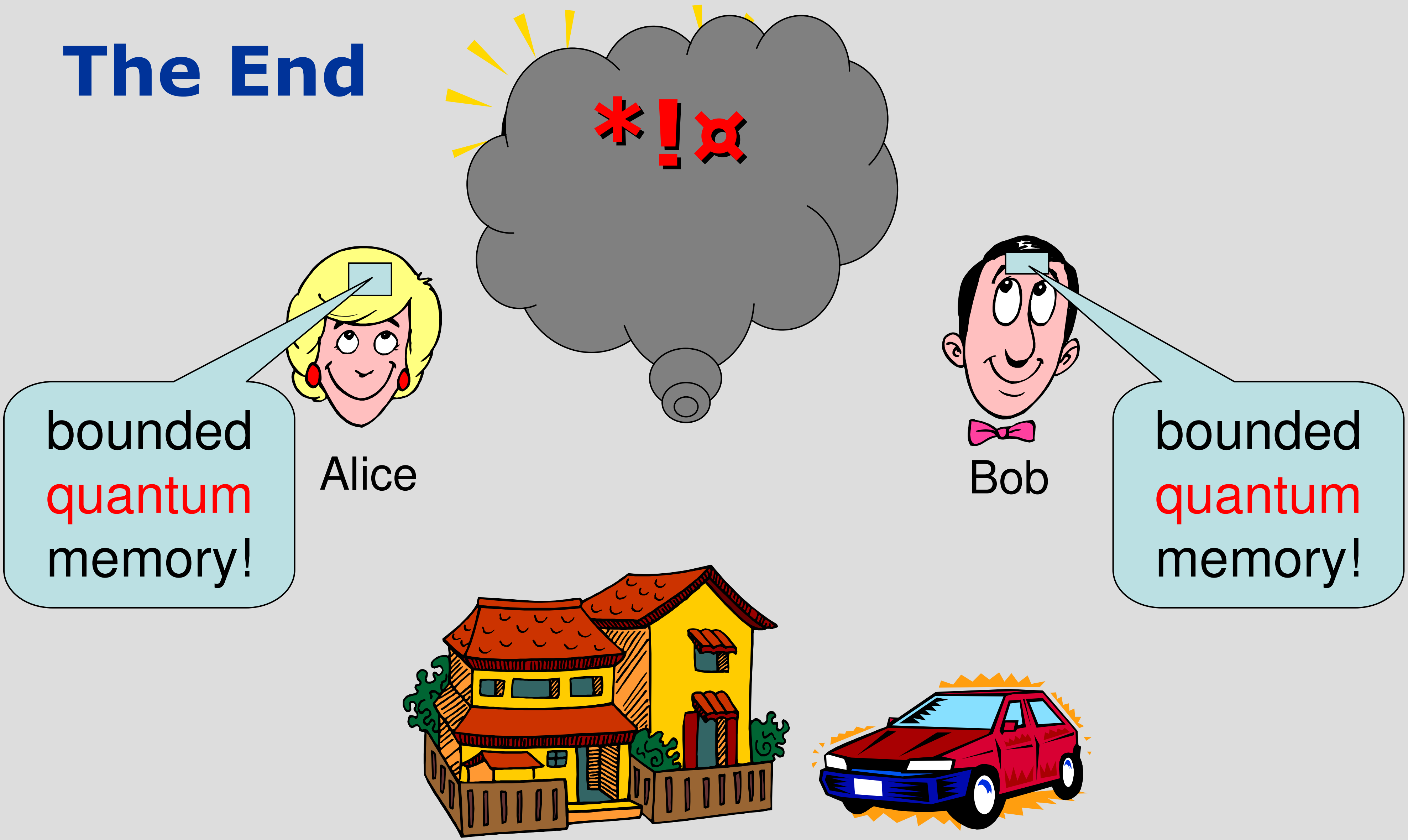
open

classically:
$\text{Memory}_{\text{cheater}} < 2 \cdot \text{Mem}_{\text{honest}}$

- perfectly hiding
- honest Alice needs *no quantum memory*
- $\text{Memory}_{\text{cheater}} < n/2 \Rightarrow$ binding

Christian Schaffner, PhD student
NF-årsfest 2005

The End

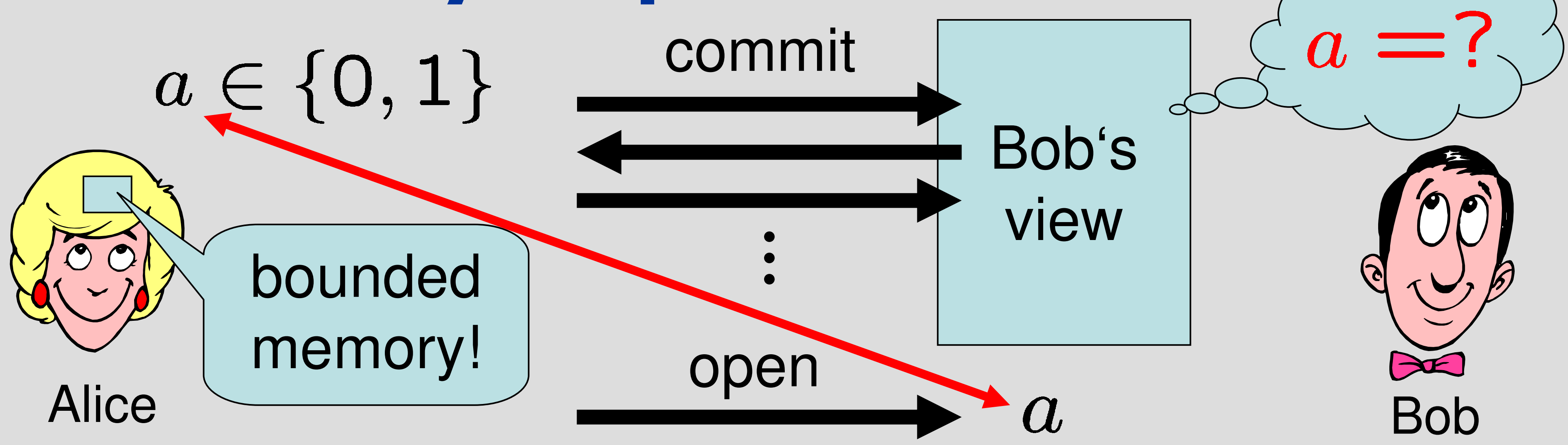


AARHUS UNIVERSITET

DAIMI – Department of Computer Science
BRICS – Basic Research in Computer Science

Christian Schaffner, PhD student
NF-årsfest 2005

Classically Impossible



- ~~hiding~~
- ~~binding~~ ✓

perfectly secure, without assumptions
- with classical communication
- with quantum communication

AARHUS UNIVERSITET
DAIMI – Department of Computer Science
BRICS – Basic Research in Computer Science
Christian Schaffner, PhD student
NF-årsfest 2005