Quantum Bit Commitment

Christian Schaffner

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

NAT-årsfest
June 3, 2005
Divorce Problems

who gets the house?

Alice

Bob
Coin-Flipping over the Telephone

It's tails, I get the house!
A Coin-Flipping Protocol

\[ a \in_R \{0, 1\} \]

\[ b \in_R \{0, 1\} \]

not random!

\[ a \neq b \]
The Solution

\[ a \in_R \{0, 1\} \]

\[ b \in_R \{0, 1\} \]

Alice

Bob

\[ a = b \]

\[ a \neq b \]
The Explanation

\[ a \in_R \{0, 1\} \]

\[ b \in_R \{0, 1\} \]

\[ a = b \]

\[ a \neq b \]
Bit-Commitment Scheme

\[ a \in \{0, 1\} \]

- important cryptographic primitive
- hiding
- binding

Alice

commit

Bob's view

open

Bob

\[ a =? \]
Particular Bit-Commitment Scheme

\[ a \in \{0, 1\} \]

- honest Alice needs: \( n \)
- cheating Alice needs: \( 2 \cdot n \)
- Memory_{cheater} < 2 \cdot Memory_{honest} \Rightarrow binding
- perfectly hiding

Bob’s view

commit to 0 (\(n\) MegaBytes)
commit to 1 (\(n\) MB)

open

Alice

Bob

\( a = ? \)
Quantum Bit-Commitment Scheme

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

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

Alice

Bob

$\alpha = \text{?}$

$n$ quantum bits

open

$	ext{Bob's view}$
The End

Alice: bounded quantum memory!

Bob: bounded quantum memory!
Classically Impossible

\[ a \in \{0, 1\} \]

- hiding
- binding

perfectly secure, without assumptions

- with classical communication
- with quantum communication

Alice

Bob

committed

open

Bob's view

a

NF-årsest 2005

Christian Schaffner, PhD student

NF-årsest 2005