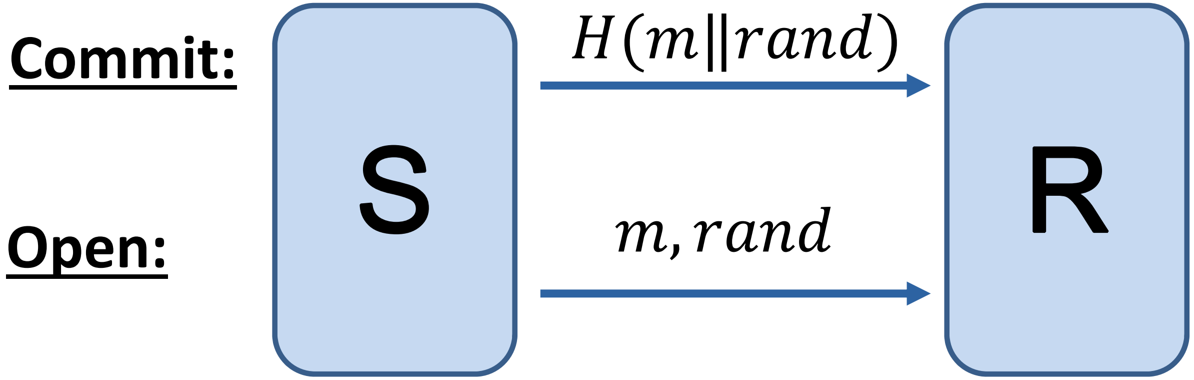
Computationally binding quantum commitments

Dominique Unruh

University of Tartu

Intro: Commitments

Motivation: Secretly fixing bets



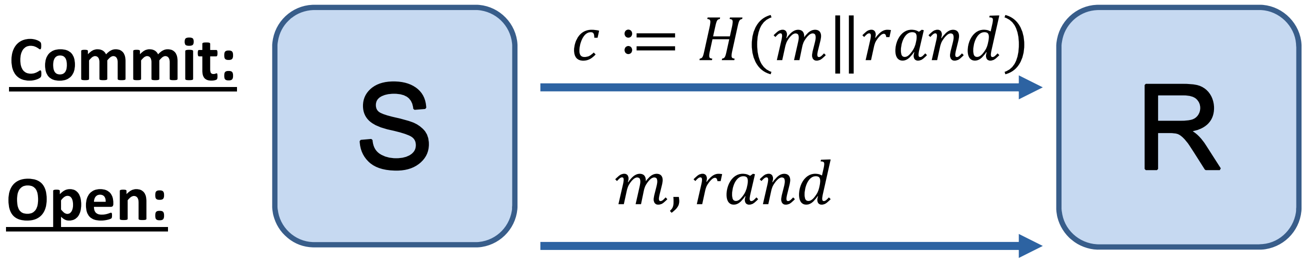
Commit:

Open:

- **Hiding:** Recipient does not learn m
- **Binding:** Sender cannot change his mind

Tricky.
This talk

How to define binding?



Commit:

Open:

S

R

$c := H(m\|rand)$

$m, rand$

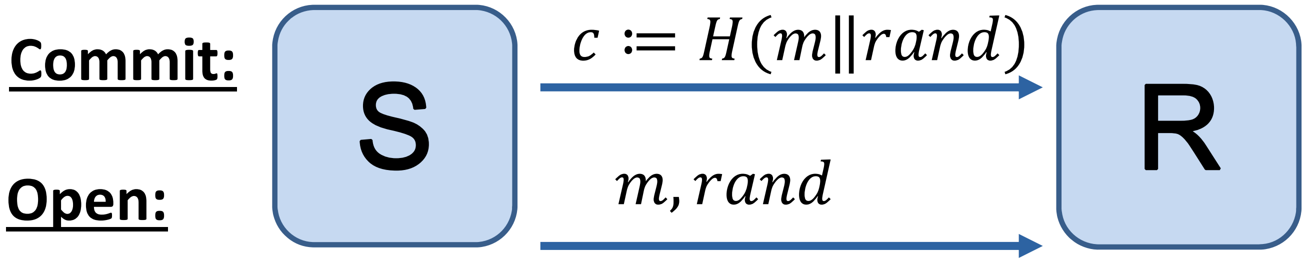
Perfectly binding:

There are no $m \neq m'$

such that $H(m\|rand) = H(m'\|rand')$
for some $rand, rand'$

Problem:
Incompatible with information-theoretical secrecy…

How to define *computational* binding?



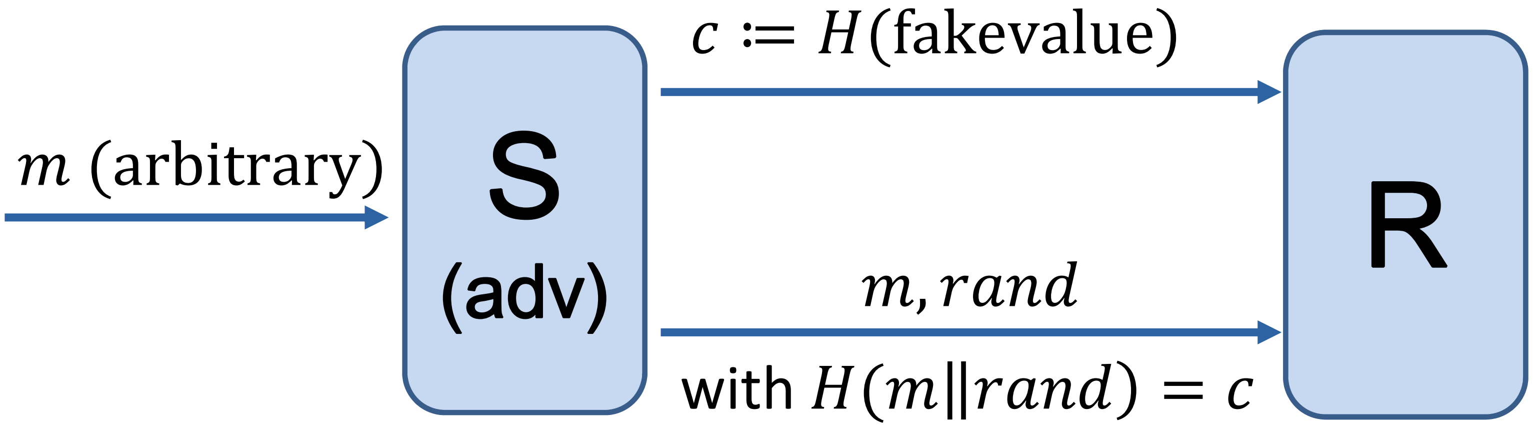
Computationally binding (classical-style):

It is computationally hard to find
$m \neq m'$ and $rand, rand'$
such that $H(m\|rand) = H(m'\|rand')$

Intuition:
Adversary cannot find out how to open two ways.

Classical-style binding: no good!

- There is a commitment scheme such that:



- But still computationally binding (classical-style)
- Reason: Adv can open arbitrarily, but not **at the same time**

[Ambainis, Rosmanis, U 2014; this work]

Computational binding: Next try

Computationally binding (typical Q def):

- Fix malicious poly-time adv S
- Let P_0 be probability that S opens as $m = 0$
- Let P_1 be probability that S opens as $m = 1$
- Then

$$P_0 + P_1 \leq 1 + \text{negligible}$$

Computational binding: Next try

Computationally binding (typical Q def):

- Fix malicious poly-time adv S
- Let P_0 be probability that S opens as $m = 0$
- Let P_1 be probability that S opens as $m = 1$
- Then

$$P_0 + P_1 \leq 1 + \text{negligible}$$

- Only works for single bit messages
- Unclear what happens if we commit to several messages $m_0, m_1, \ldots, m_n$
- Works bad with rewinding proofs

More definitions

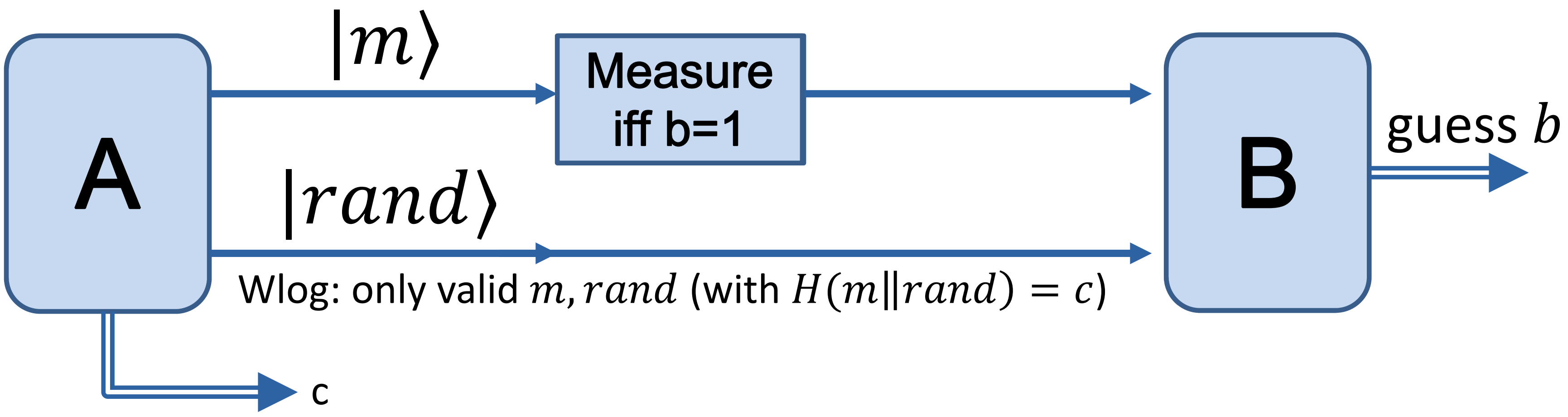
- Crépeau, Dumais, Mayers, Salvail, 2004
  Computational collapse of quantum state with application to oblivious transf
- UC-comm
- Damgård, ffner 2009
  Improving th mmit-and-open (dual-m
- Damgård, Fehr, Salvail, 2004
  Zero-Knowledge Proofs and String Commitments Withstanding Quantum Attacks

None work well with rewinding proofs

(and other problems)

Towards our def

- Reformulating perfect binding:

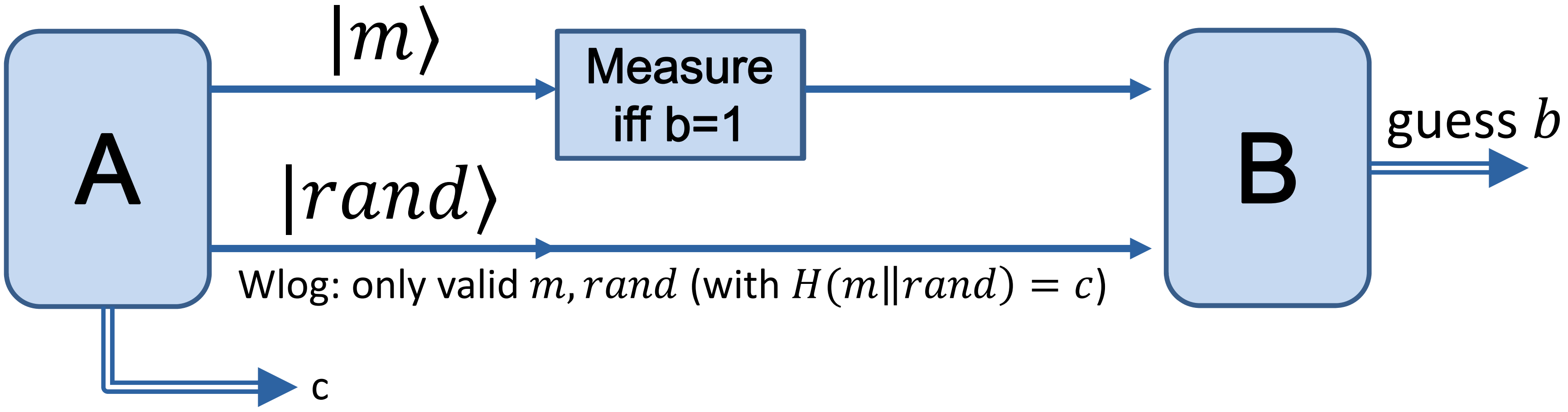


Wlog: only valid $m, rand$ (with $H(m\|rand) = c$)

- Perfect binding **iff** no superposition in $|m\rangle$ register
- Perfect binding **iff** measurement has no effect
- Perfect binding **iff** B cannot guess b (better than ½)

Collapse binding (new def)

Perfect binding **iff** B cannot guess b (better than ½)



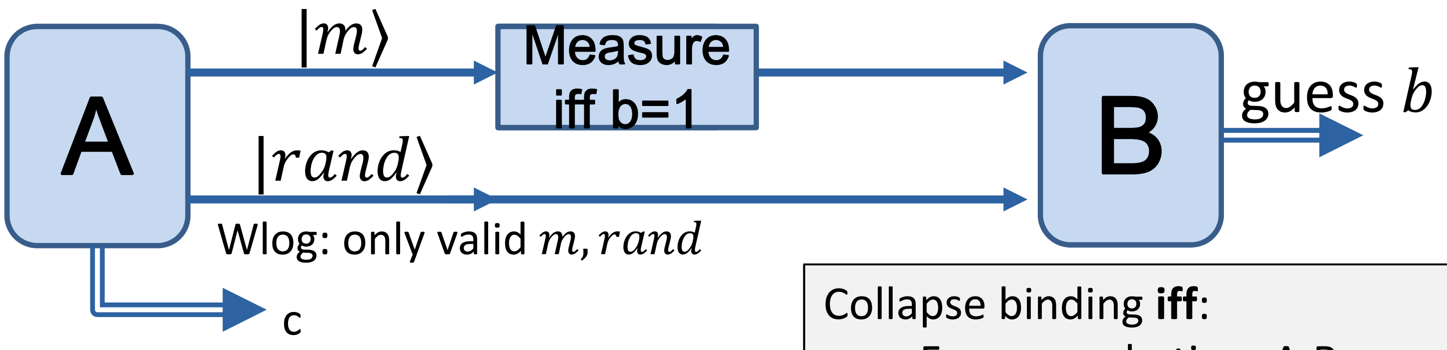
Wlog: only valid $m, rand$ (with $H(m\|rand) = c$)

"Collapse binding" **iff**:

For any poly-time A,B,

B cannot guess b (better than ${}^1/_2$ + negligible)

Facts about new def



Wlog: only valid $m, rand$

Collapse binding **iff**:

For any poly-time A,B,

B cannot guess b (better than $^1/_2 +$ negligible)

- Works well with rewinding
  - We analyzed arguments of knowledge
- Multi-bit m, composes in parallel
- For random oracle H, natural constructions work

Open problems

- Relationship between the definitions
- Constructions without random oracle
  - We have sketches
- Analyse protocols based on collapse-binding commitments
  - Done: Arguments of knowledge
  - Open: OT protocol, e.g., [BBCS91]

I thank for your attention

European Union
European Social Fund

Investing in your future

ARCHIMEDES

DoRa

European Union
Regional Development Fund

Investing in your future

EXCS
ESTONIAN COMPUTING

This research was supported
by European Social Fund's
Doctoral Studies and
Internationalisation
Programme DoRa