Cryptography In the Bounded Quantum-Storage Model

joint work with Ivan Damgård, Serge Fehr and Louis Salvail
(accepted at FOCS 2005)

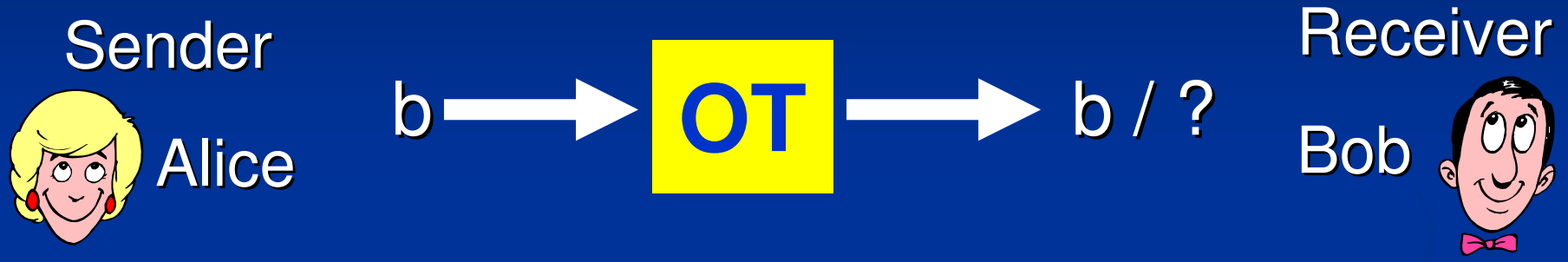
Christian Schaffner, BRICS
University of Århus, Denmark

CS-QIC , University of Calgary
Monday, August 8th 2005

Agenda

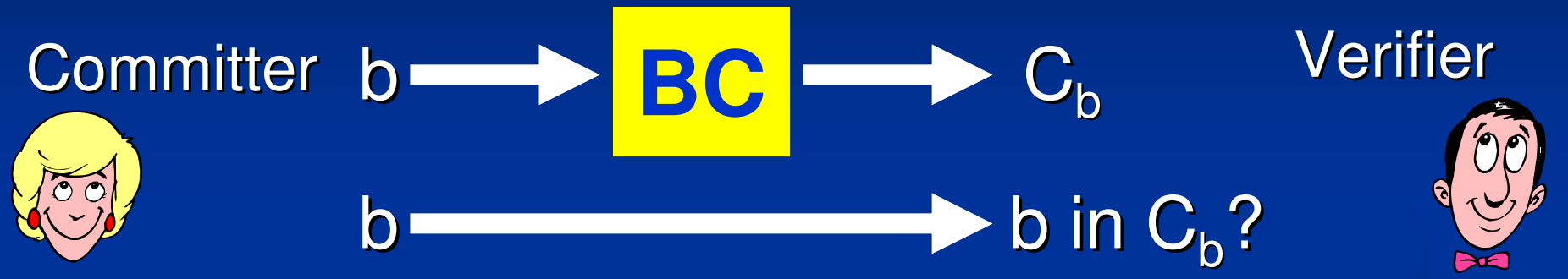
- “Known” Results
- Protocol for Oblivious Transfer
- Security Proof
- Bit Commitment
- Practicality Issues
- Open Problems

Classical 2-party primitives: Rabin Oblivious Transfer



- **correct:** For honest Alice and Bob, Bob gets the bit b with probability ½
- **oblivious:** Even if Bob is dishonest, he does not get information about b with probability ½
- **private:** Even if Alice is dishonest, she does not learn, whether Bob received the bit or not.

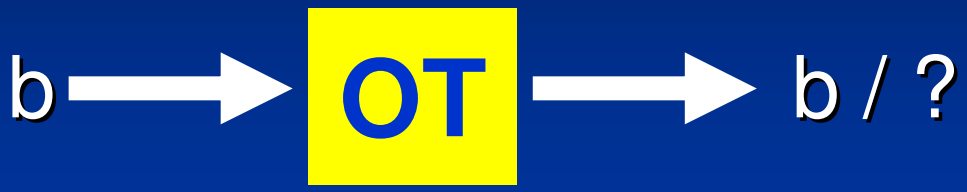
Classical 2-party primitives: Bit Commitment



- **correct:** BC allows Alice to commit to a bit b. Later, she can open C_b to Bob.
- **hiding:** Even if Bob is dishonest, he does not get information on b from C_b.
- **binding:** Even if Alice is dishonest, she cannot open C_b to another value than b.

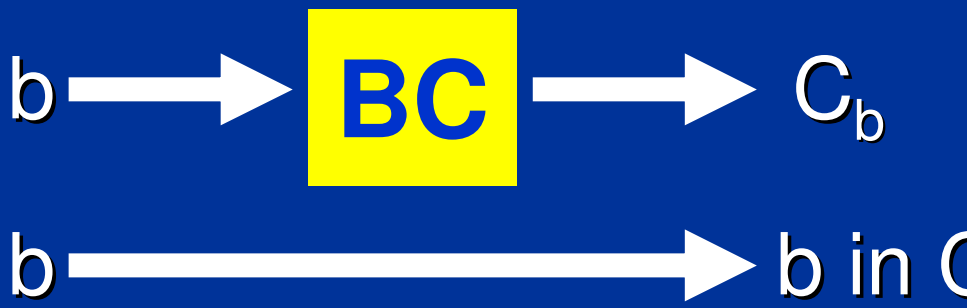
Classical 2-party primitives: Relations

Oblivious Transfer



- oblivious
- private

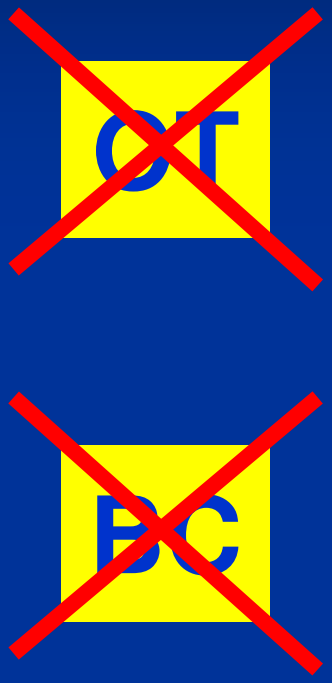
Bit Commitment



- hiding
- binding

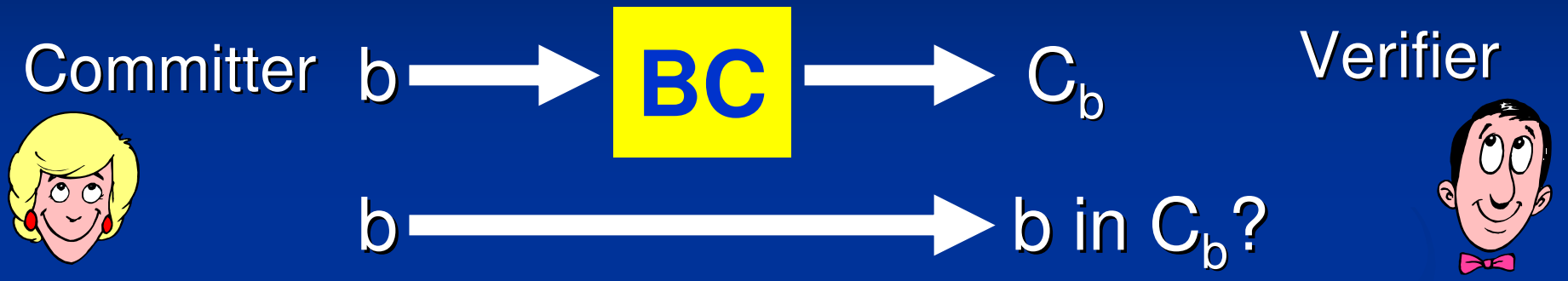
- **OT** $\Rightarrow$ **BC**, **OT** $\geq$ **BC**
- **OT** is complete for two-party cryptography

Known Impossibility Results



- In the classical unconditionally secure model without further assumptions

Classical 2-party primitives: Bit Commitment



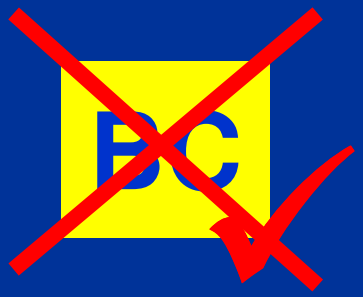
- **hiding:** Even if Bob is dishonest, he does not get information on b from C_b.
- **binding:** Even if Alice is dishonest, she cannot open C_b to another value than b.

Known Impossibility Results

- In the classical unconditionally secure model without further assumptions

- In the unconditionally secure model **with quantum communication**
  [Mayers97, Lo-Chau97]

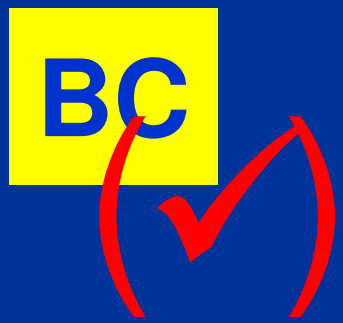
Three Ways Out



- Bound computing power (schemes based on complexity assumptions)
- Noisy communication [e.g. CrépeauMorozovWolf04]
- ➪ **Physical limitations**

e.g. bounded memory size

Classical Bounded-Storage Model



- random string which players try to store
- a memory bound applies at a specified moment
- protocol for OT [DHRS, TCC04]:
  memory size of honest players: k
  memory of dishonest players: $<k^2$
- Tight bound [DM, EC04]
- can be **improved** by allowing **quantum communication**

Quantum Bounded-Storage Model

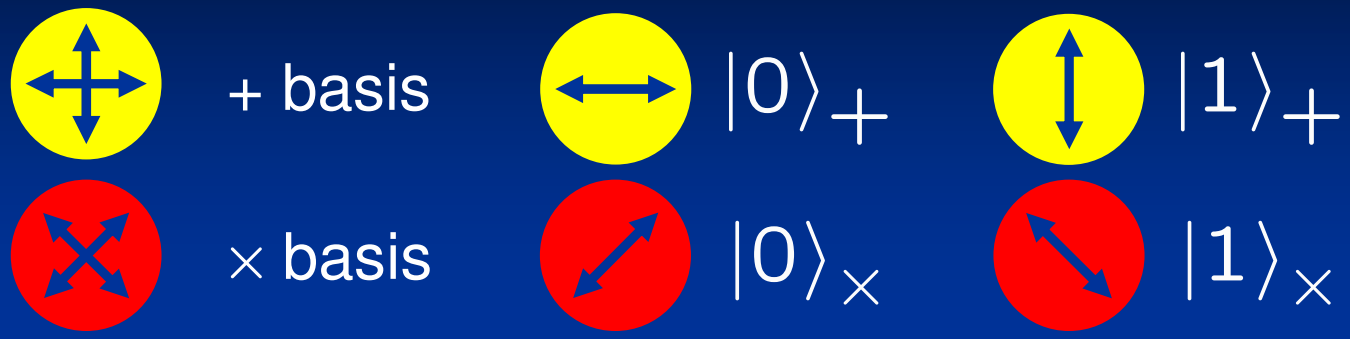
- quantum memory bound applies at a specified moment
- besides that, players are unbounded (in time and space)
- **unconditional secure** against adversaries with quantum memory of less then **half of the transmitted qubits** (honest players **do not need quantum** memory **at all**)

honest players:	0	k
dishonest players:	$<n/2$	$<k^2$
ratio:	∞	**k**

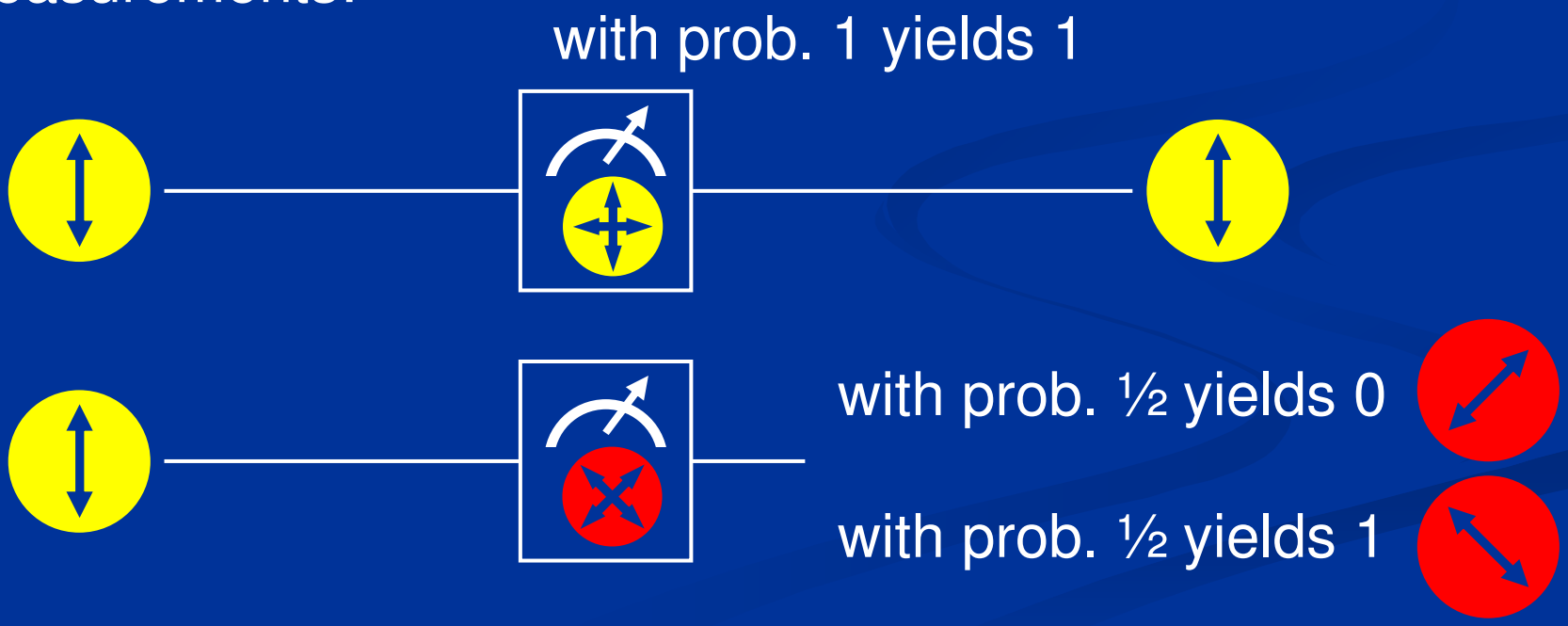
Agenda

- ✓ Known Results
- **Protocol for Oblivious Transfer**
- Security Proof
- Bit Commitment
- Practicality Issues
- Open Problems

Quantum Mechanics I



Measurements:



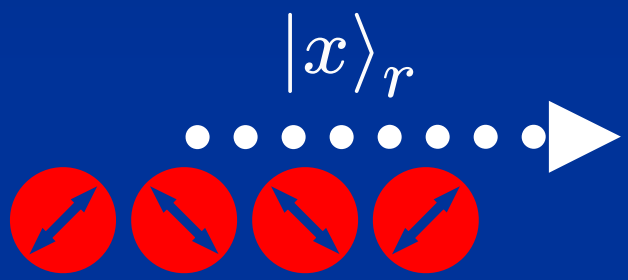
Quantum Oblivious Transfer

Alice $b \in \{0,1\}$

$r \in_R \{+,\times\}$

$x \in_R \{0,1\}^n$

0110...



Bob

$r' \in_R \{+,\times\}$

obtains x' by measuring all qubits in basis r'

0110...

memory bound: store < n/2 qubits

CS1

$h \in_R H_n$

$s = b \oplus h(x)$

r, h, s

gets $b = s \oplus h(x')$ if $r = r'$

Example: honest players

CS1

h is two-universal and BINARY

Christian Schaffner; 24.02.2005

Quantum Oblivious Transfer II

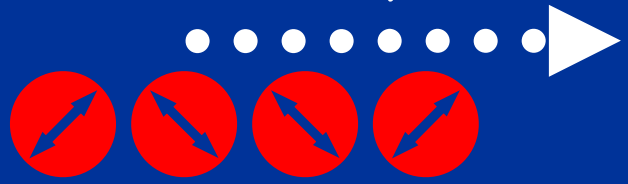
Alice

$r \in_R \{+, \times\}$

$x \in_R \{0,1\}^n$

0110...

$|x\rangle_r$



Bob

$r' \in_R \{+, \times\}$

obtains x' by measuring all qubits in basis r'

0011...

memory bound: store < n/2 qubits

$h \in_R H_n$

$s = b \oplus h(x)$

r, h, s

$x \neq x' \Rightarrow h(x'), h(x)$ indep

gets $b = s \oplus h(x')$

$b \stackrel{?}{=}$ if $r = r'$

honest players? ✓

private? ✓

Obliviousness against dishonest Bob?

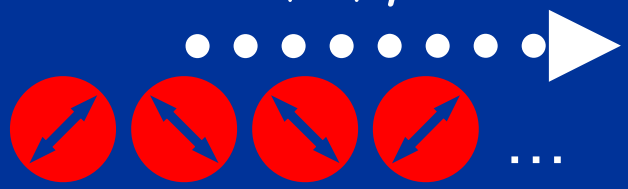
Alice

$r \in_R \{+, \times\}$

$x \in_R \{0,1\}^n$

0110...

$|x\rangle_r$



...

Bob

$r' \in_R \{+, \times\}$

store all qubits!

obtains x' by

measuring all qubits

in the right bases

11...

memory bound: store < n/2 qubits

$h \in_R H_n$

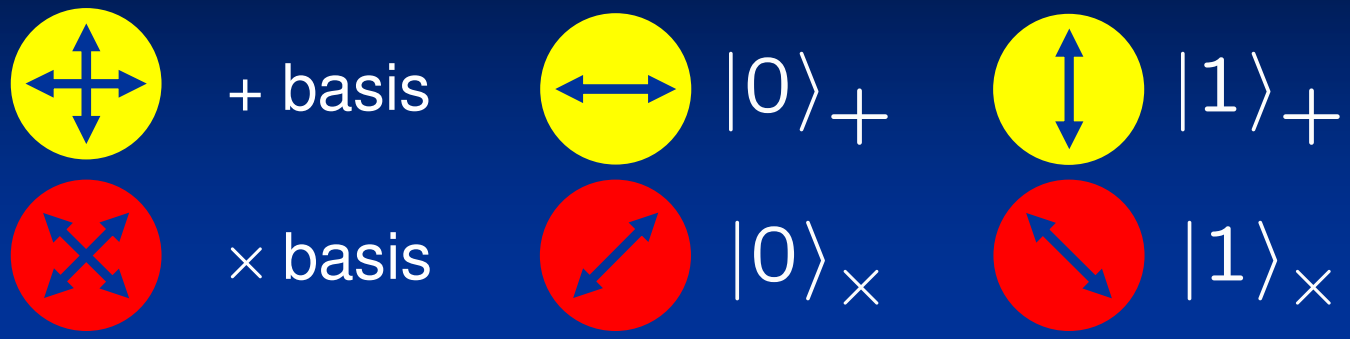
$s = b \oplus h(x)$

r, h, s

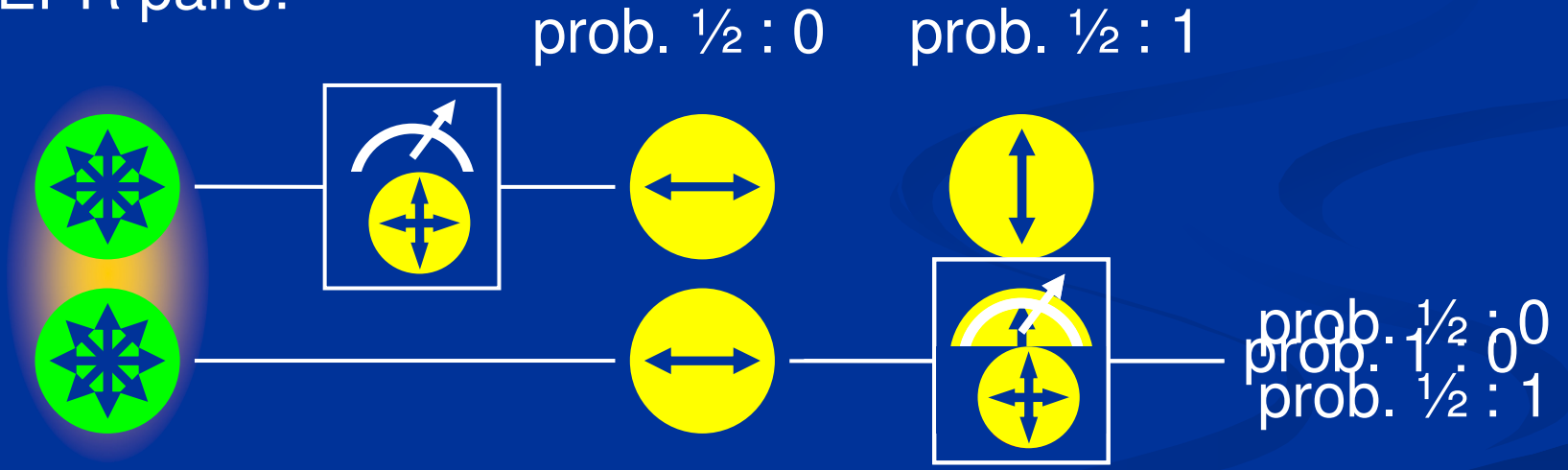
gets $b = s \oplus h(x')$

if $r = r'$

Quantum Mechanics II



EPR pairs:

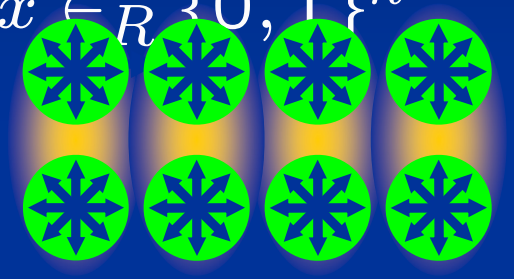


Proof of Obliviousness: Purification

Alice

$r \in_R \{+, \times\}$

$x \in_R \{0,1\}^n$



$|x\rangle_r$

Bob

store all qubits!

memory bound: store < n/2 qubits

$h \in_R H_n$

$s = b \oplus h(x)$

r, h, s

gets $b = s \oplus h(x')$

if $r = r'$

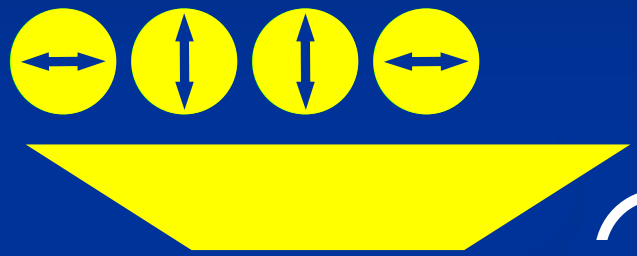
Proof of Obliviousness: Purification II

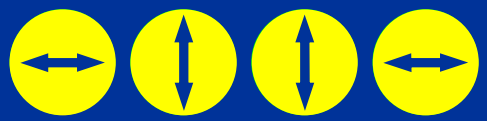
Alice

$r \in_R \{+, \times\}$

Bob

store all qubits!





memory bound: store < n/2 qubits

$x^0 \in_R \{0,1\}^{n^0}$

$h \in_R H_n$

$s = b \oplus h(x)$

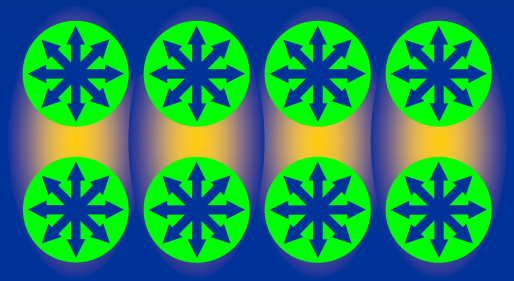
r, h, s

gets $b = s \oplus h(x')$ if $r = r'$

Proof of Obliviousness: EPR-Version

Alice **Bob**

store all qubits!



memory bound: store < n/2 qubits

$r \in_R \{+, \times\}$

$h \in_R H_n$

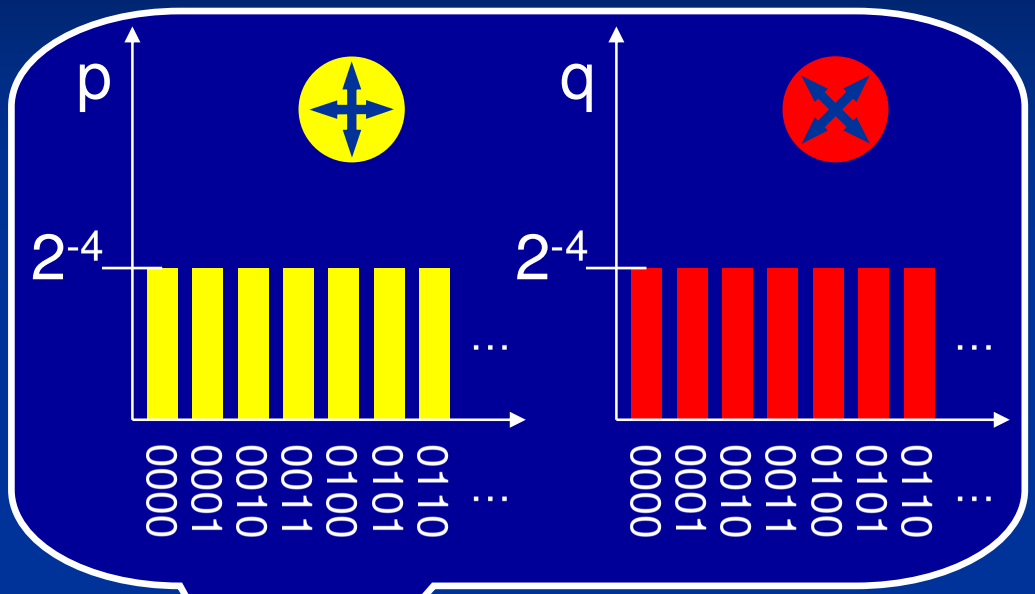
$s = b \oplus h(x)$

r, h, s

gets $b = s \oplus h(x')$
if $r = r'$

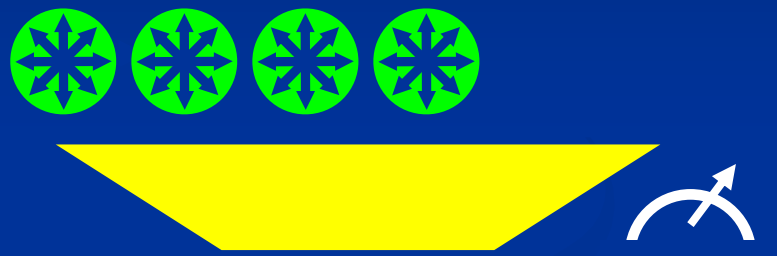
Proof of Obliviousness: Distributions

Alice



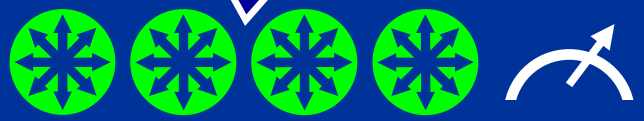
Bob

store all qubits!



memory bound: store < n/2 qubits

$r \in_R \{+, \times\}$



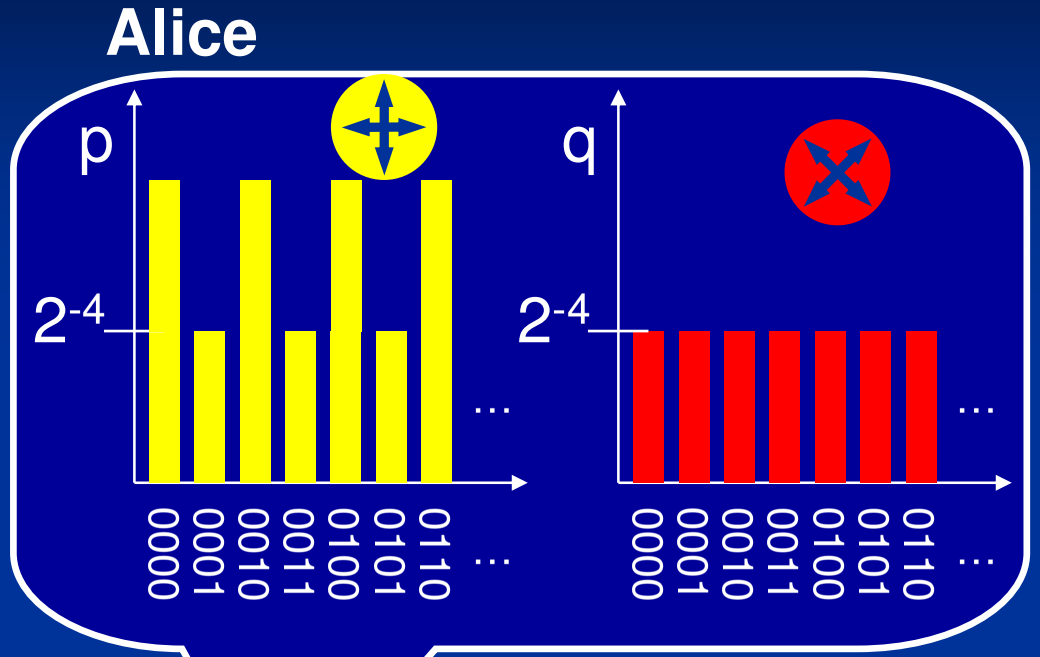
$h \in_R H_n$

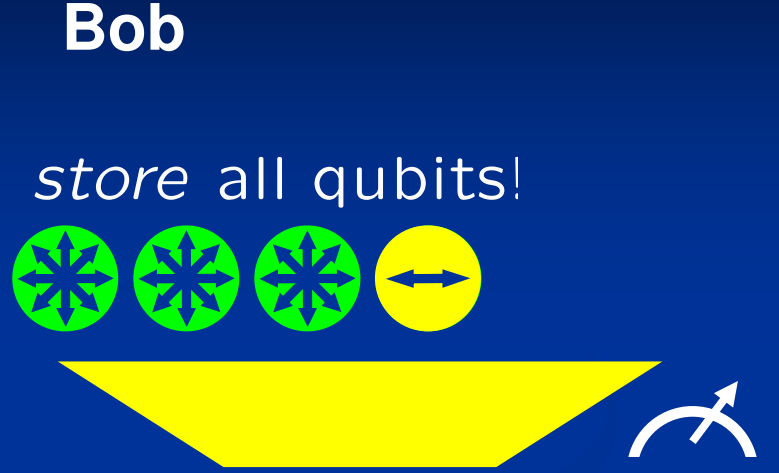
$s = b \oplus h(x)$

r, h, s

gets $b = s \oplus h(x')$ if $r = r'$

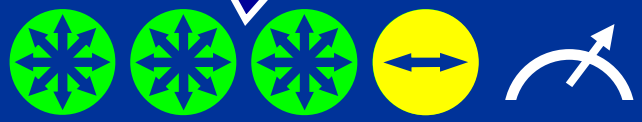
Proof of Obliviousness: Example





memory bound: store < n/2 qubits

$r \in_R \{+, \times\}$



$h \in_R H_n$

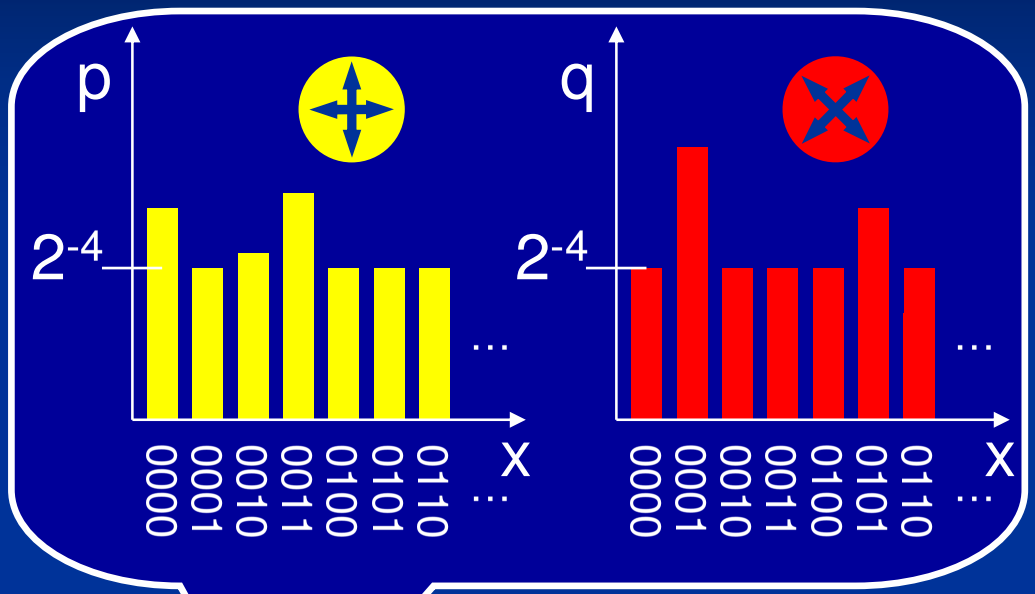
$s = b \oplus h(x)$

r, h, s

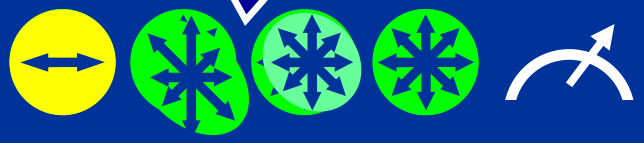
gets $b = s \oplus h(x')$ if $r = r'$

Proof of Obliviousness: Distributions II

Alice



$r \in_R \{+, \times\}$



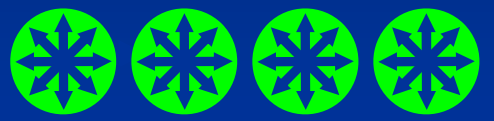
$h \in_R H_n$

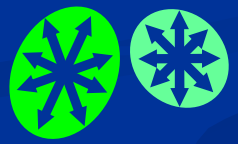
$s = b \oplus h(x)$

r, h, s

Bob

store all qubits!



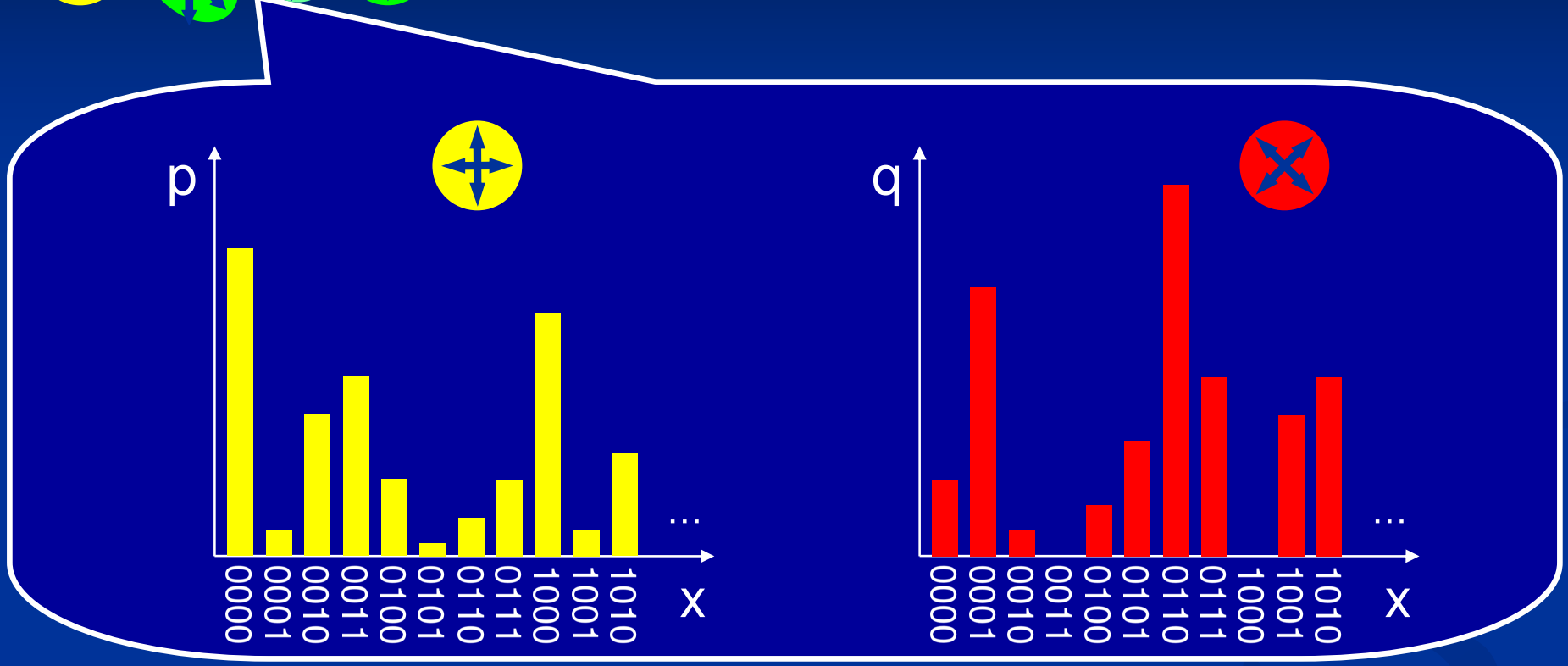


001…

memory bound: store < n/2 qubits

gets $b = s \oplus h(x')$
if $r = r'$

Proof of Obliviousness: Goal

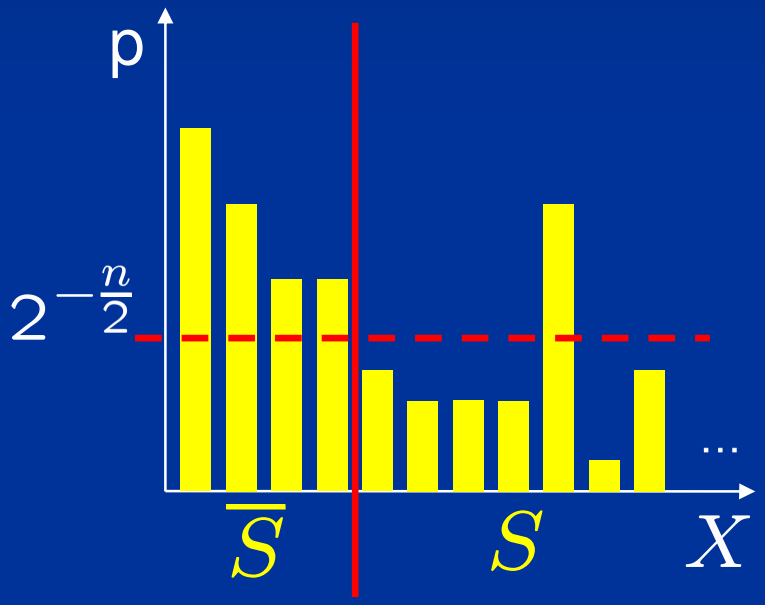


However Bob prepares his memory 001…

and the distributions p and q, he cannot guess h(x) in **both bases simultaneously** ⇒ **oblivious**

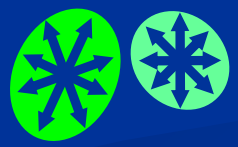
Privacy Amplification

Privacy Amplification against Quantum Adversaries
[Renner & König, TCC 2005]



X a RV over $\{0,1\}^n$

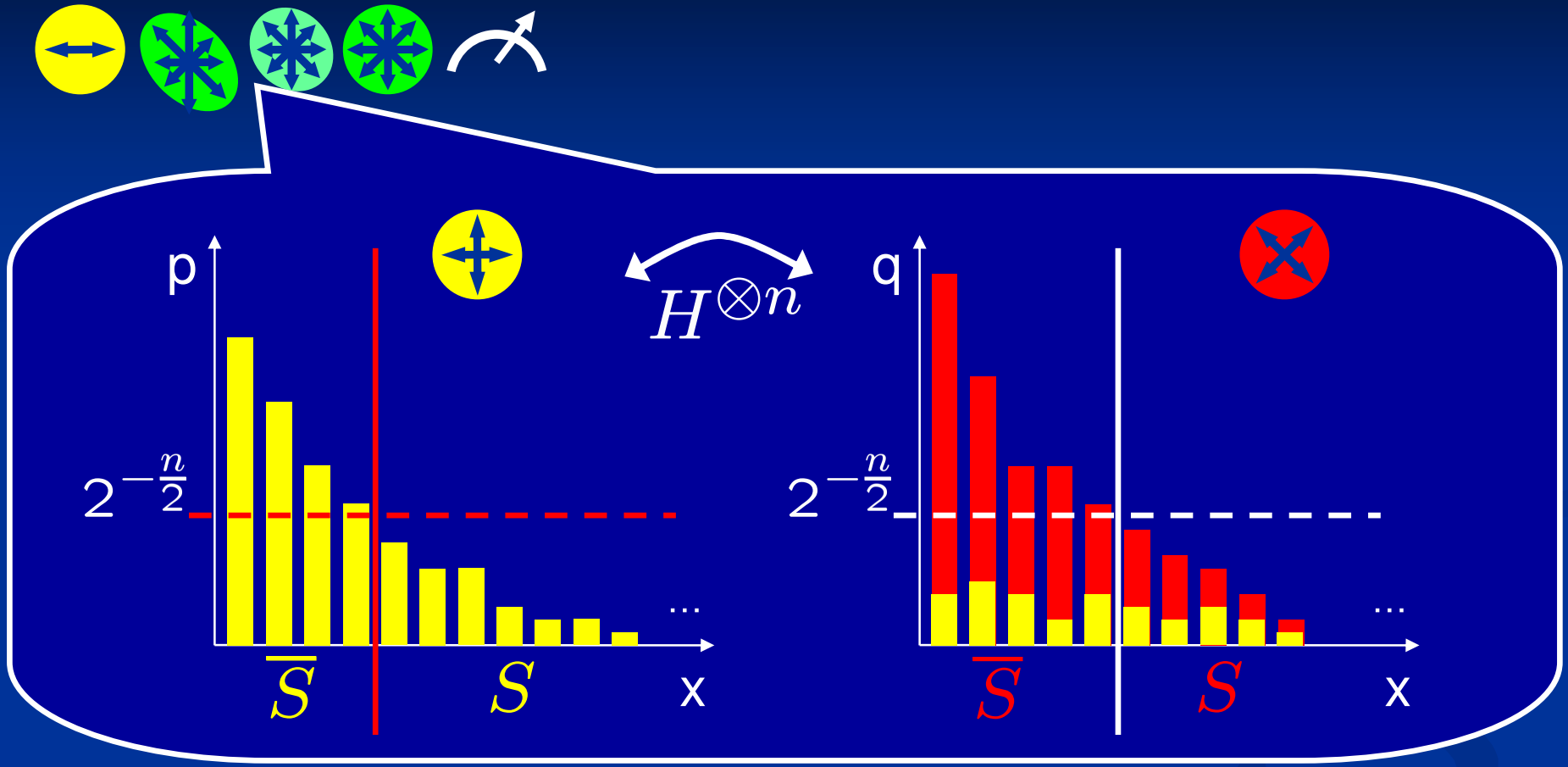
memory of $< \frac{n}{2}$ qubits

$X \longmapsto$  ...

$h : \{0,1\}^n \to \{0,1\}$
guess $h(X)$ given qmemory!

Theorem: If $-\log_2(p_\infty(X)) = H_\infty(X) > \frac{n}{2}$, then Bob has only negligible knowledge about $h(X)$.

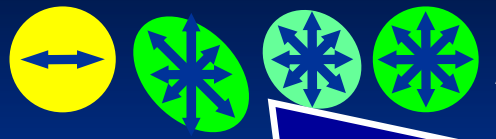
Obliviousness: Uncertainty Relation

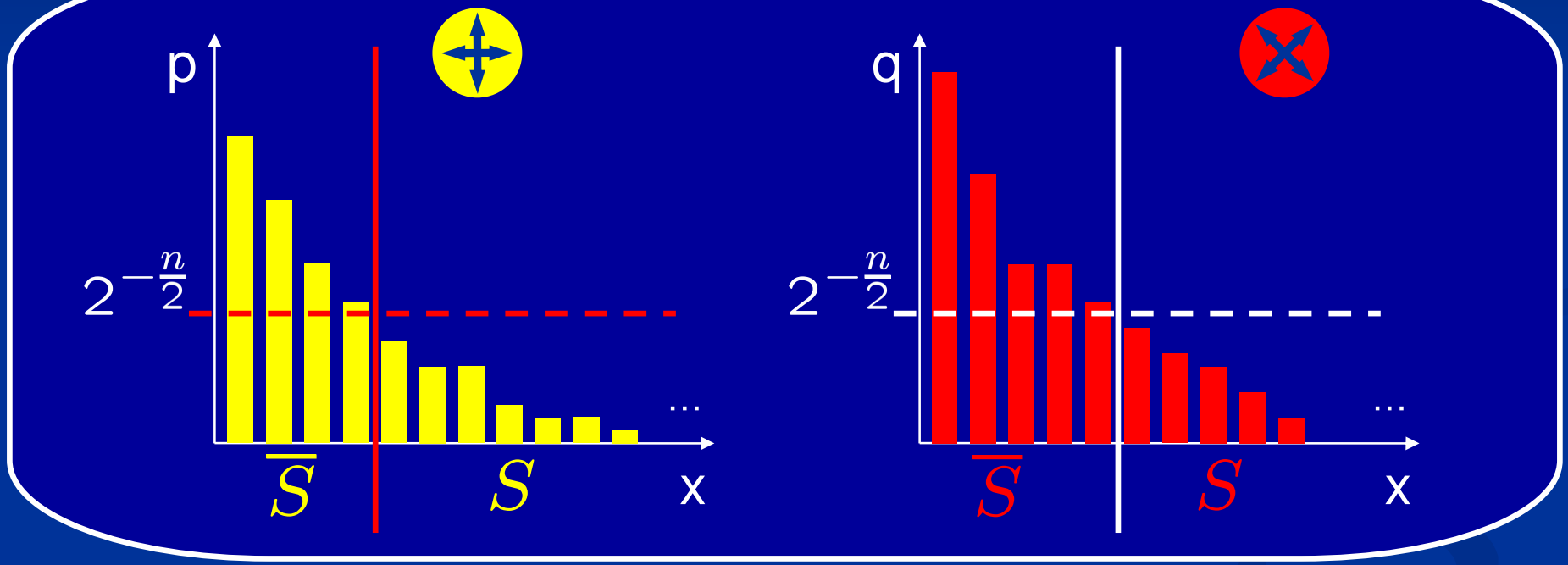


$$p(S) + negl(n) \geq q(\overline{S}) = 1 - q(S)$$

Theorem: $p(S) + q(S) \geq 1$

Proof of Obliviousness: Finale





$p(S) + q(S) \geq 1$ $\qquad$ $\mathcal{E} := \{x \in S\}$

$\Rightarrow \Pr[\mathcal{E}] = \frac{1}{2}\{p(S) + q(S)\} \geq \frac{1}{2}$

Proof of Obliviousness: Recap

Alice

$r \in_R \{+, \times\}$

$x \in_R \{0,1\}^n$

Bob

store all qubits!

memory bound: store ≤ n/2 qubits

$h \in_R H_n$

$s = b \oplus h(x)$

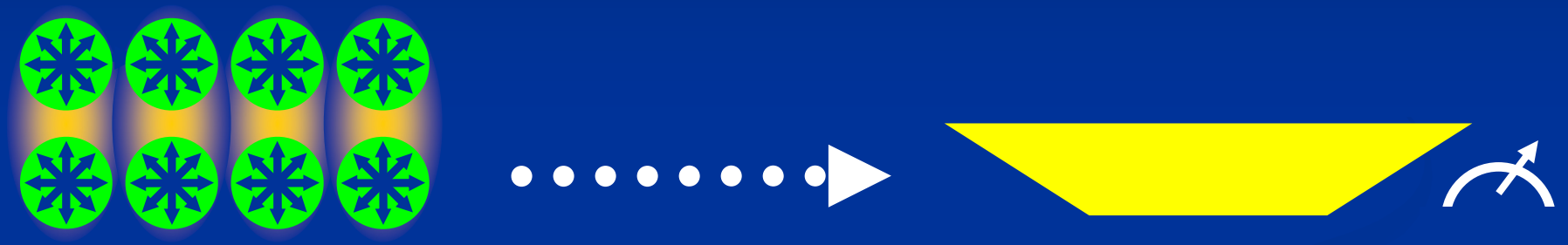
r, h, s

gets $b = s \oplus h(x')$ if $r = r'$

Proof of Obliviousness: Recap II

Alice **Bob**

store all qubits!



memory bound: store ≤ n/2 qubits

$\in_R \{+, \times\}$

$h \in_R H_n$

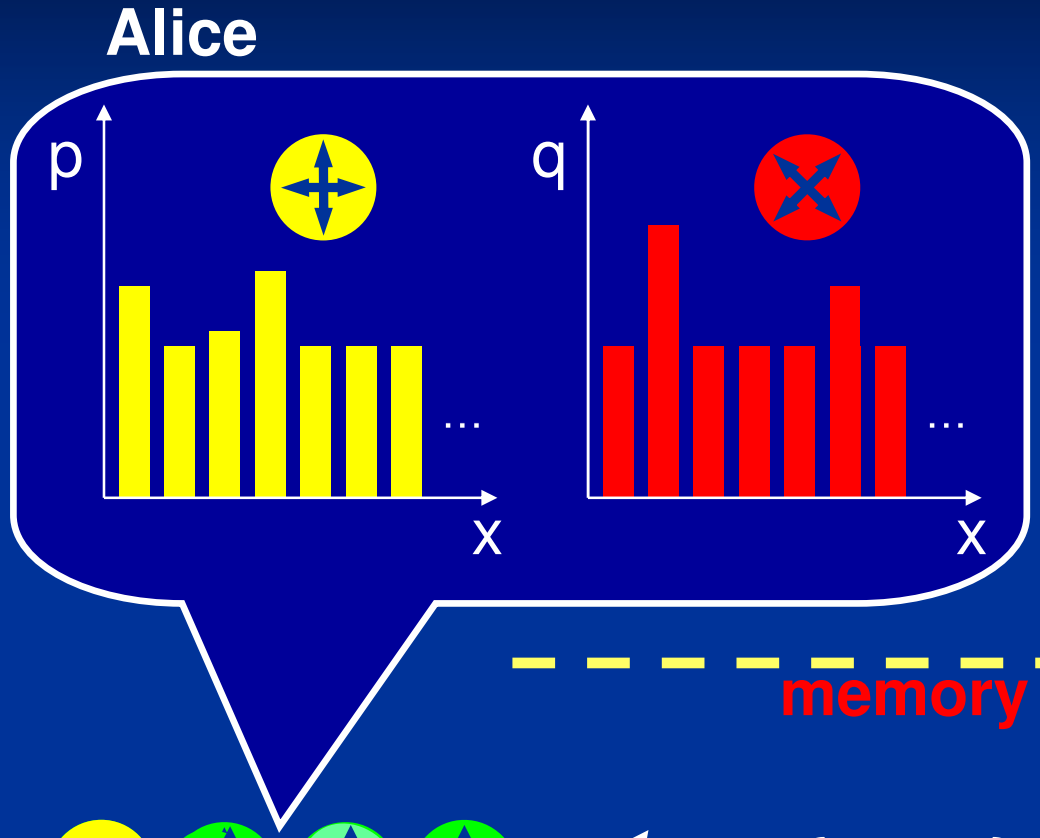
$s = b \oplus h(x)$

r, h, s

gets $b = s \oplus h(x')$

if $r = r'$

Proof of Obliviousness: Recap III

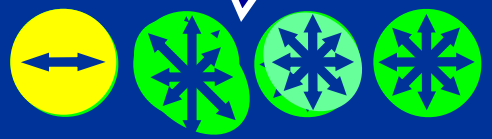


Bob

store all qubits!

001…

memory bound: store ≤ n/2 qubits



$\in_R \{+, \times\}$

$h \in_R H_n$

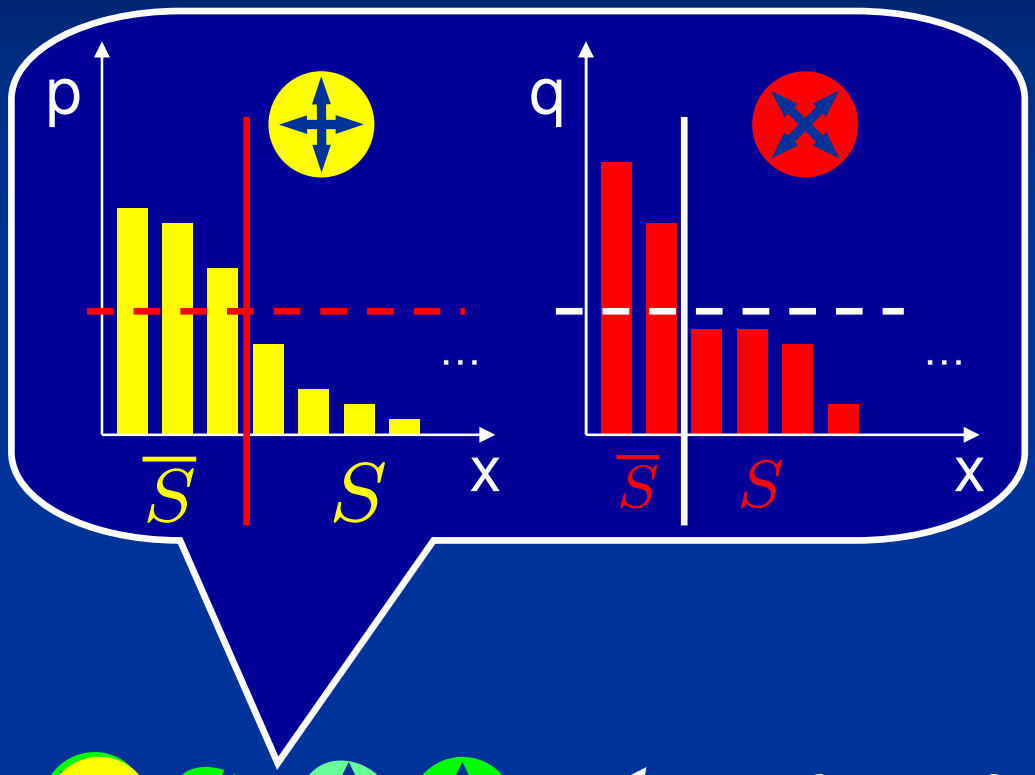
$s = b \oplus h(x)$

r, h, s

gets $b = s \oplus h(x')$ if $r = r'$

Proof of Obliviousness: Recap IV

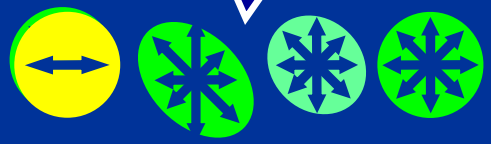
Alice



Bob

$\mathcal{E} := \{x \in S\}$
with $\Pr[\mathcal{E}] \geq \frac{1}{2}$

□



$\in_R \{+, \times\}$

$h \in_R H_n$

$s = b \oplus h(x)$

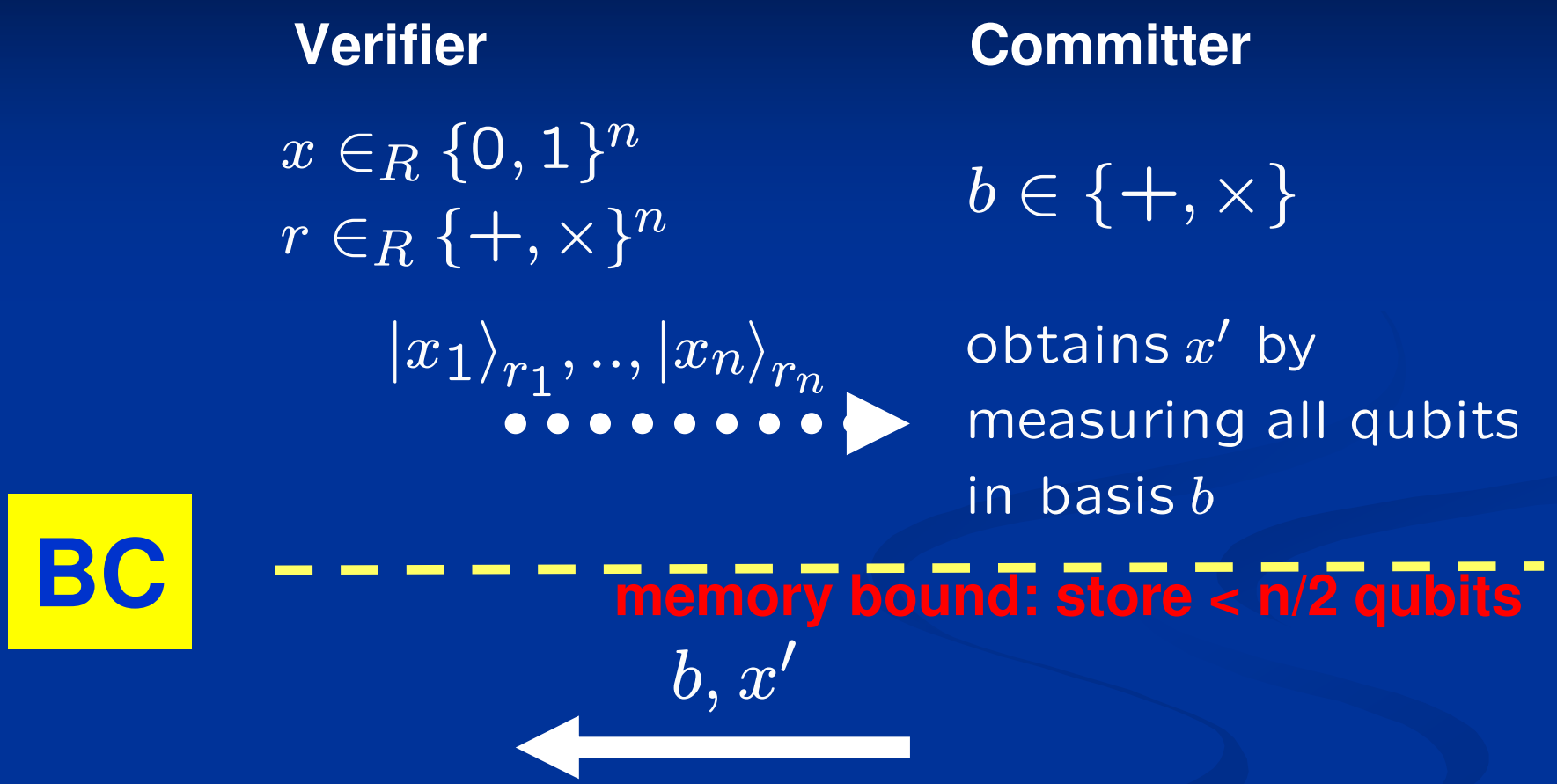
r, h, s

gets $b = s \oplus h(x')$
if $r = r'$

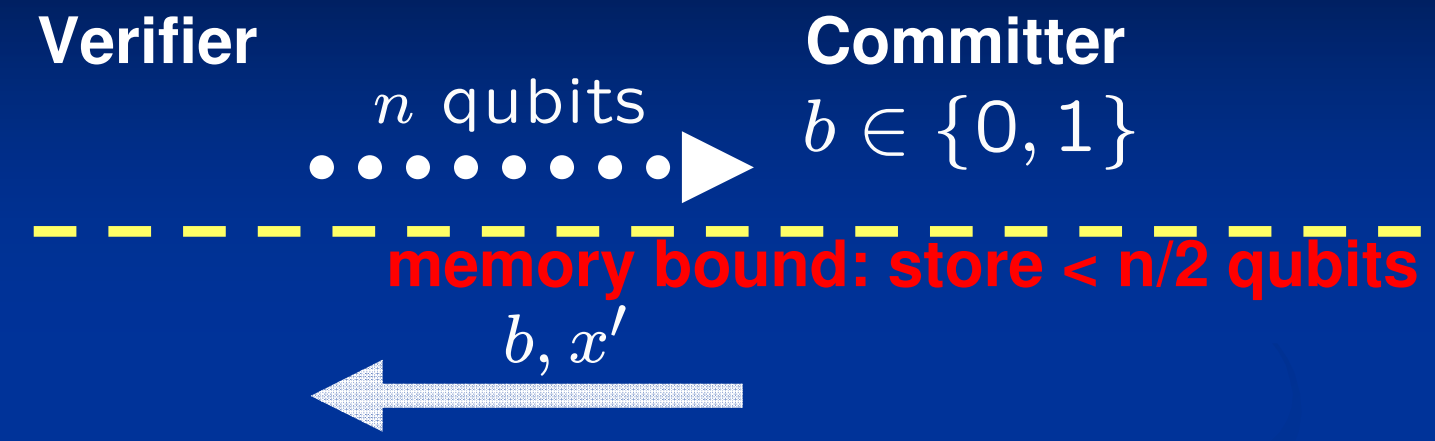
Agenda

- ✓ Known Results
- ✓ Protocol for Oblivious Transfer
- ✓ Security Proof
- **Bit Commitment**
- Practicality Issues
- Open Problems

Quantum Bit Commitment



Quantum Bit Commitment II



BC

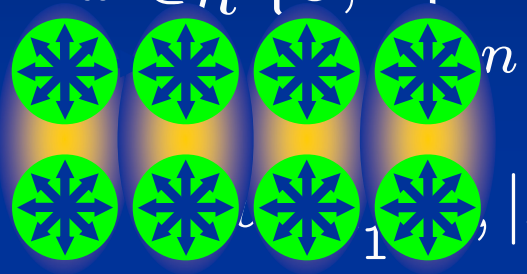
- one round
- non-interactive (commit by receiving)
- unconditionally hiding
- unconditionally binding:
  - classically: $\text{Mem}_{\text{dis}} < 2 \cdot \text{Mem}_{\text{hon}}$
  - **quantum:** $\text{Mem}_{\text{dis}} < n / 2$

Binding Property: Proof Idea

Verifier

Committer

$x \in_R \{0,1\}^n$



store all qubits!
$b \in \{+, \times\}$

measuring all qubits
in basis b

BC

memory bound: store < n/2 qubits

b, x'

accepts, if $x_i = x'_i$
where $r_i = b$

Agenda

- ✓ Known Results
- ✓ Protocol for Oblivious Transfer
- ✓ Security Proof
- ✓ Bit Commitment
- **Practicality Issues**
- Open Problems

Practicality Issues

OT

BC

With today's technology, we

- **can** transmit quantum bits
  - encode bits in the correct basis
  - send them over optical fibers
  - receive and measure them
- **cannot store** them for longer than a few milliseconds

Problems:

- imperfect sources (multi-pulse emissions)
- transmission errors

Practicality Issues II

Our protocols can be modified to

- **resist** attacks based on multi-photon emissions
- tolerate (quantum) **noise**

➔ Well within reach of **current technology** and **unconditionally secure** as long as nobody can store large amounts of quantum bits.

Open Problems and Next Steps

- Other flavors of OT:
  e.g. 1-out-of-2 Oblivious Transfer, String-OT, …
- Better memory bounds

- Composability? What happens to the memory bound?
- Better uncertainty relations for more MUB
- …

Quantum 1-2-OT

Alice $b_0, b_1 \in \{0,1\}$

$r \in_R \{+,\times\}^n$

$x \in_R \{0,1\}^n$

Bob $c \in \{0,1\}$

$r' := [+,\times]_c$

$|x_1\rangle_{r_1}, .., |x_n\rangle_{r_n}$ ⟶

obtains x' by measuring all qubits in basis r'

---

memory bound: store < 0.4n qubits

$h_0, h_1 \in_R H_{n/2}$

$s_0 = b_0 \oplus h_0(x_+)$

$s_1 = b_1 \oplus h_1(x_\times)$

r, h_0, h_1

s_0, s_1 ⟶

gets $b_c = s_c \oplus h_c(x'_{r'})$

Summary

Protocols for OT and BC that are

- efficient
- non-interactive
- **unconditionally secure** against adversaries with bounded quantum memory
- practical:
  - honest players do not need quantum memory
  - fault-tolerant

Questions and Comments?