Cryptography In the Bounded Quantum-Storage Model

joint work with Ivan Damgård, Serge Fehr and Louis Salvail

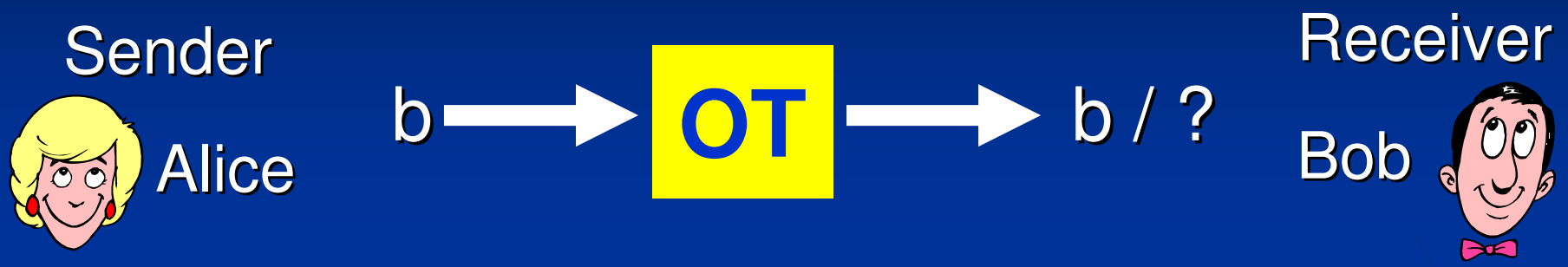
Christian Schaffner, BRICS
University of Århus, Denmark

9th workshop on QIP 2006, Paris
Tuesday, January 17th 2006

Agenda

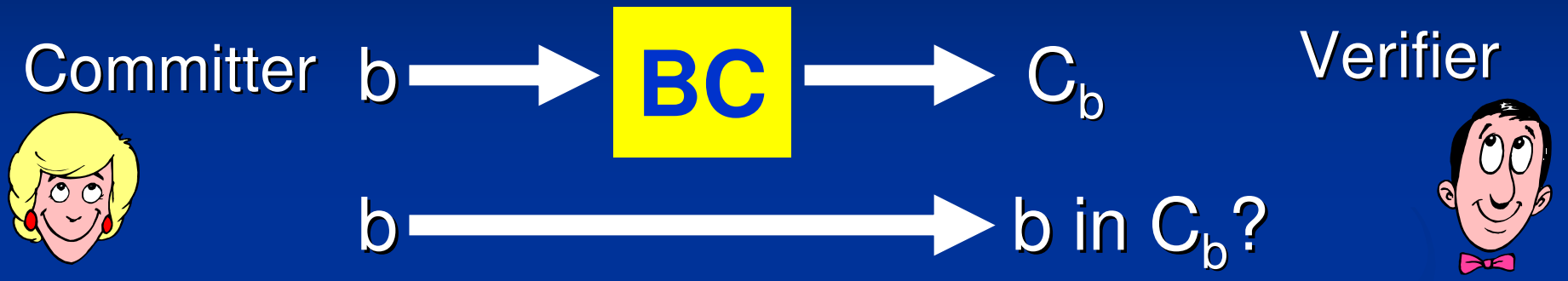
- Two-Party Crypto Primitives
- Protocol for Oblivious Transfer
- Security Proof
- Protocol for Bit Commitment
- Practicality Issues
- Open Problems

Classical 2-party primitives: Rabin Oblivious Transfer



- **correct:** For honest Alice and Bob, Bob gets the bit b with probability ½.
- **sender-private:** If Alice is honest, (cheating) Bob does not get information about b with probability bigger than ½.
- **receiver-private:** If Bob is honest, (cheating) Alice does not learn, whether Bob received the bit or not.

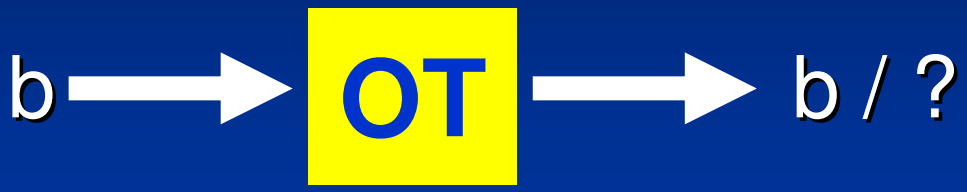
Classical 2-party primitives: Bit Commitment



- **correct:** BC allows Alice to commit to a bit b. Later, she can open C_b to Bob.
- **hiding:** If Alice is honest, (cheating) Bob does not get information on b from C_b.
- **binding:** If Bob is honest, (cheating) Alice cannot open C_b to a bit b' ≠ b.

Classical 2-party primitives: Relations

Oblivious Transfer



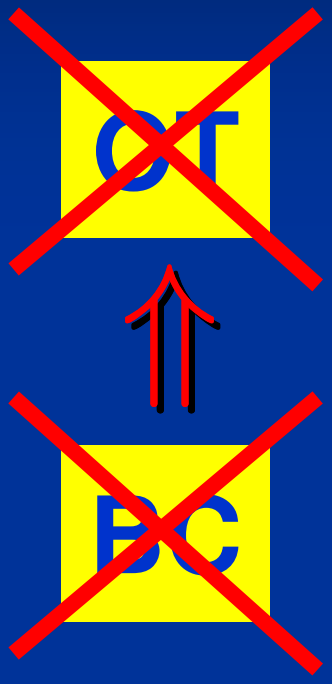
- sender-private
- receiver-private

Bit Commitment

- hiding
- binding

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

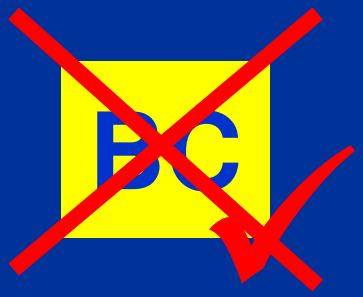
Known Impossibility Results



- In the classical unconditionally secure model without further assumptions

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

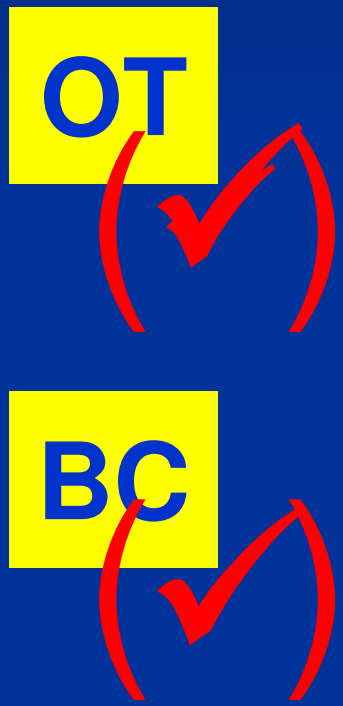
Three Ways Out



- Bound computing power (schemes based on complexity assumptions)
- Noisy communication [CrépeauKilian88, Crépeau97, …]
- **Physical limitations**

e.g. bound memory size of the players

Classical Bounded-Storage Model
[Maurer92]



- long random string in the sky which players try to store
- a memory bound applies at a specified moment (string disappears) CS3
- protocol for OT [CCM98, DHRS04]:
  memory size of honest players: k
  memory of dishonest players: $<k^2$
- Tight bound [DM04]
- can be **improved** by allowing **quantum communication**

CS3

Cachin Crepeau Marcil
Christian Schaffner; 13.01.2006

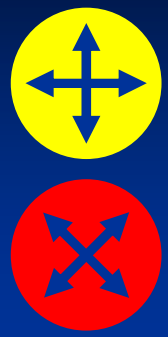
Bounded Quantum-Storage Model

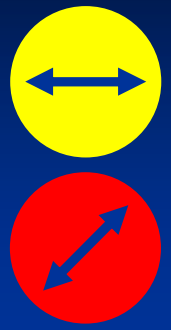
- quantum memory bound applies at a specified moment
- besides that, players are unbounded (in time and space)
- **unconditional security** against adversaries with quantum memory of less then **half of the transmitted qubits**
- honest players **do not need quantum memory at all**
- honest players: 0 k
  dishonest players: $<n/2$ $<k^2$

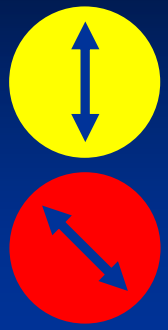
Agenda

- ✓ Two-Party Crypto Primitives
- **Protocol for Oblivious Transfer**
- Security Proof
- Protocol for Bit Commitment
- Practicality Issues
- Open Problems

Quantum Notation


+ basis


$|0\rangle_+$


$|1\rangle_+$

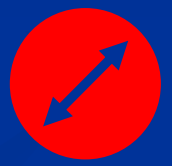
$\times$basis

$|0\rangle_\times$

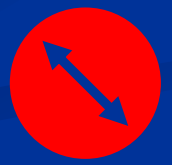
$|1\rangle_\times$

Measurements:

with prob. ½ yields 0



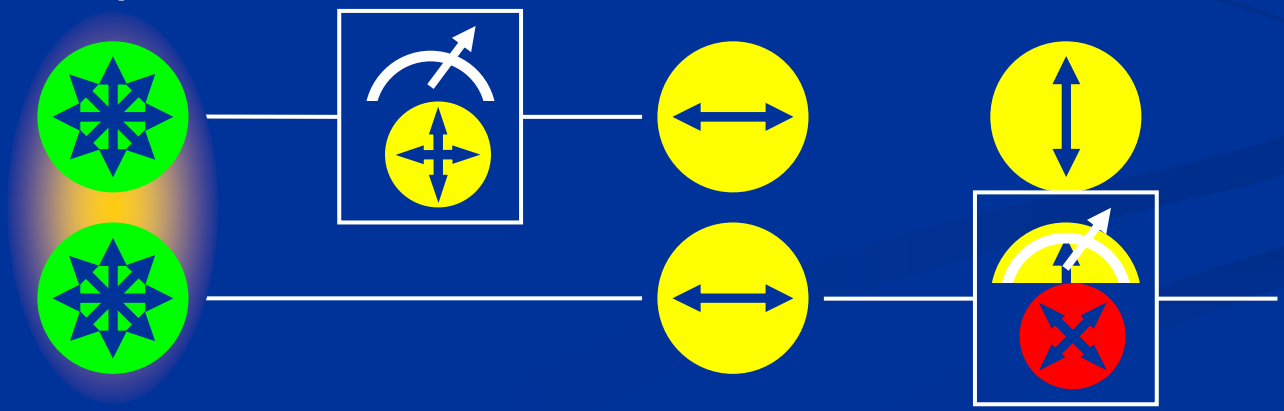
with prob. ½ yields 1



EPR pairs:

prob. ½ : 0

prob. ½ : 1



prob. ½ : 0

prob. ½ : 1

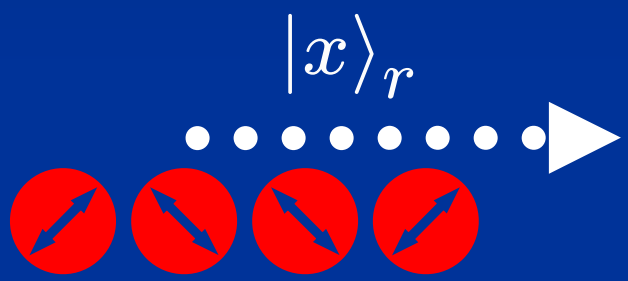
Quantum Protocol for OT

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...

[Wiesner70]

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

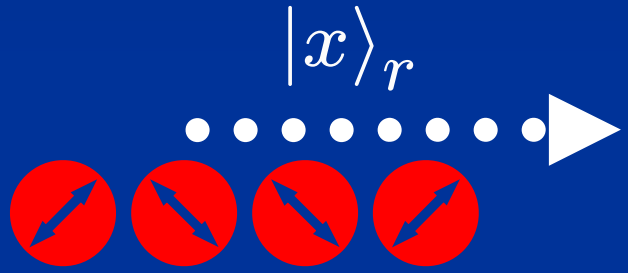
Quantum Protocol for OT II

Alice

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

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

0110...



Bob

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

obtains x' by measuring all qubits in basis r'

0011...

memory bound: store < n/2 qubits

$h \in_R H_n$

$s = b \oplus h(x)$

r, h, s

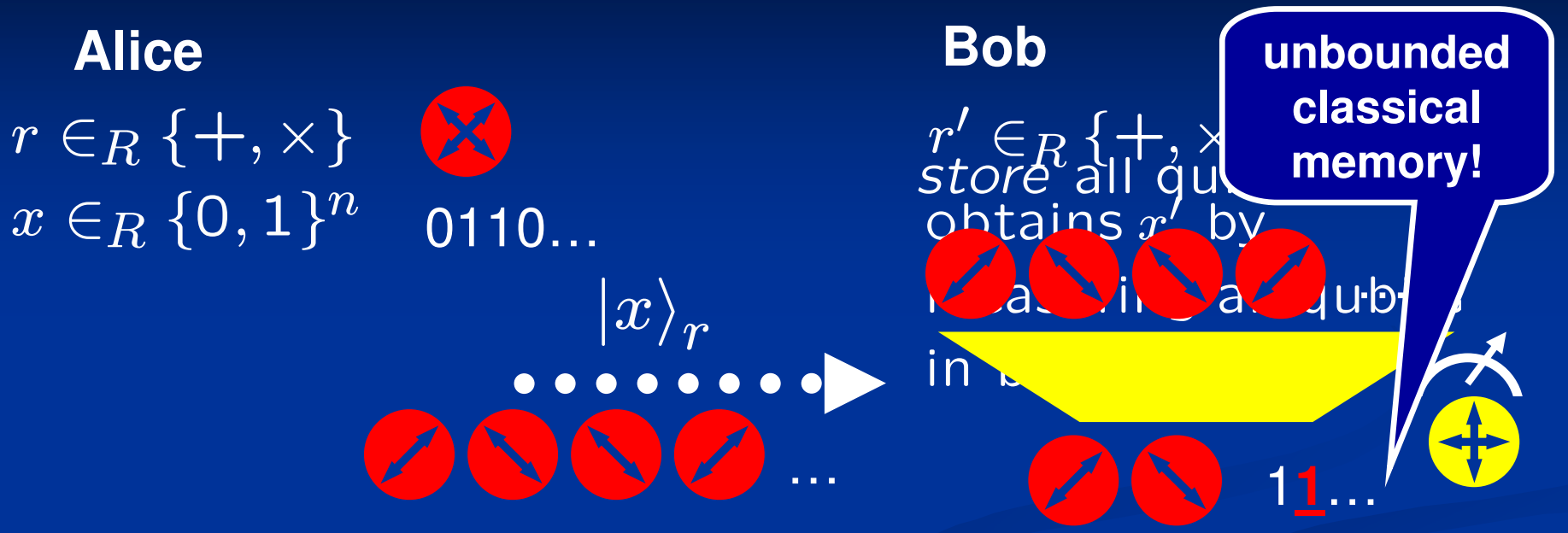
$x \neq x' \Rightarrow h(x'), h(x)$ indep

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

honest players? ✓

receiver-private? ✓

Sender-privacy against dishonest Bob?



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

$b =$? if $r = r'$

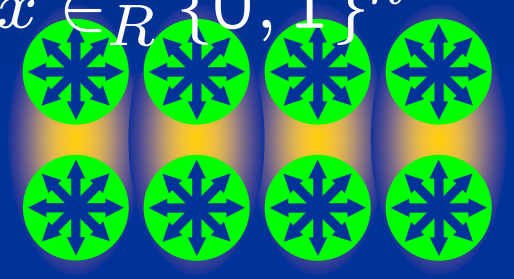
Proof of Sender-Privacy: Purification

[Ekert91]

Alice

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

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



$|x\rangle_r$

Bob

store all qubits!

memory bound: store < n/2 qubits

$h \in_R H_n$

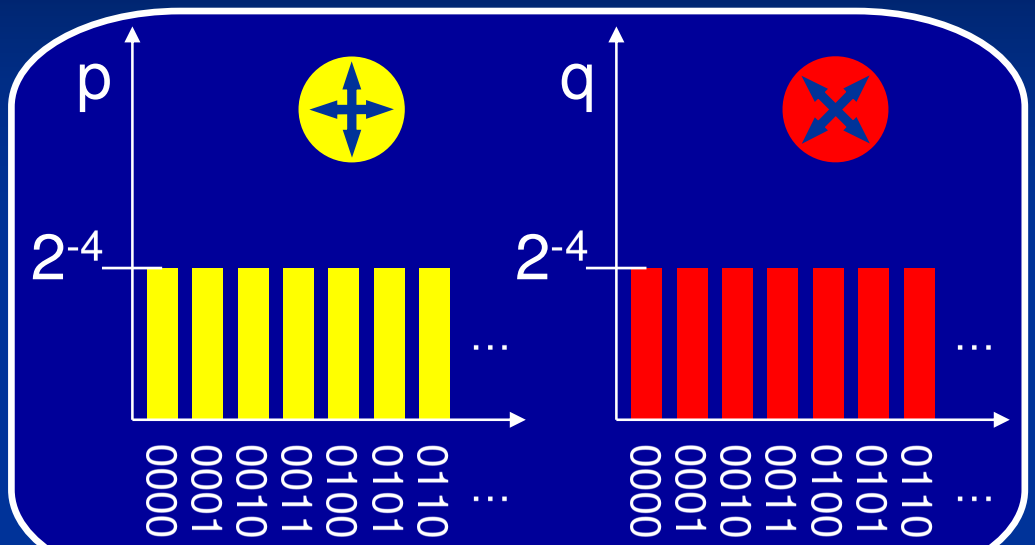
$s = b \oplus h(x)$

r, h, s

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

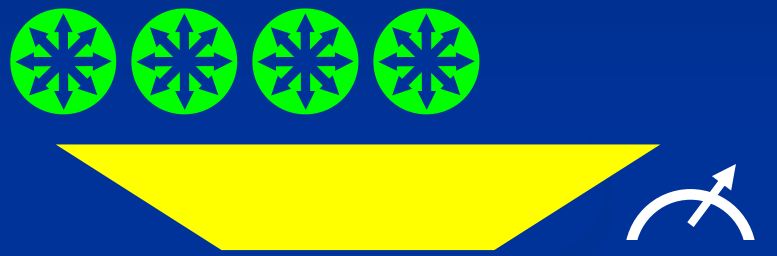
Proof of Sender-Privacy: Distributions

Alice



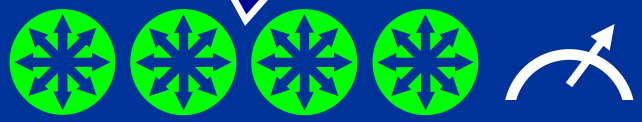
Bob

store all qubits!



memory bound: store < n/2 qubits

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



$h \in_R H_n$

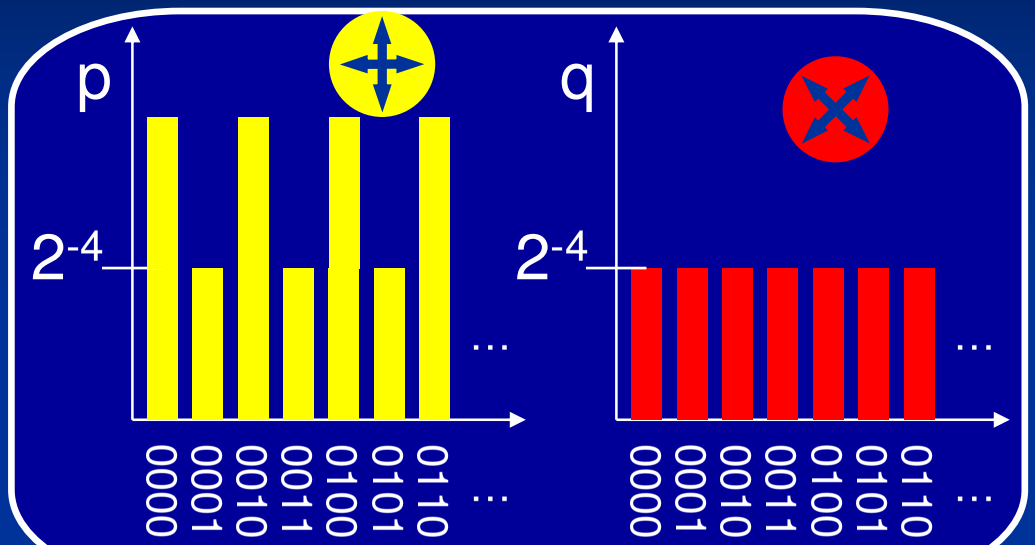
$s = b \oplus h(x)$

r, h, s

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

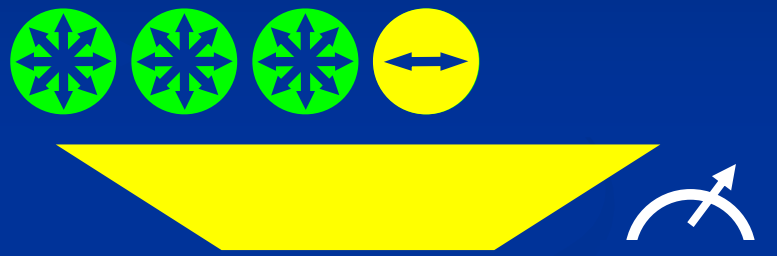
Proof of Sender-Privacy: Example

Alice



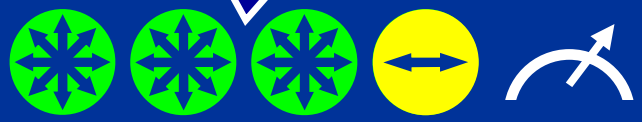
Bob

store all qubits!



memory bound: store < n/2 qubits

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



$h \in_R H_n$

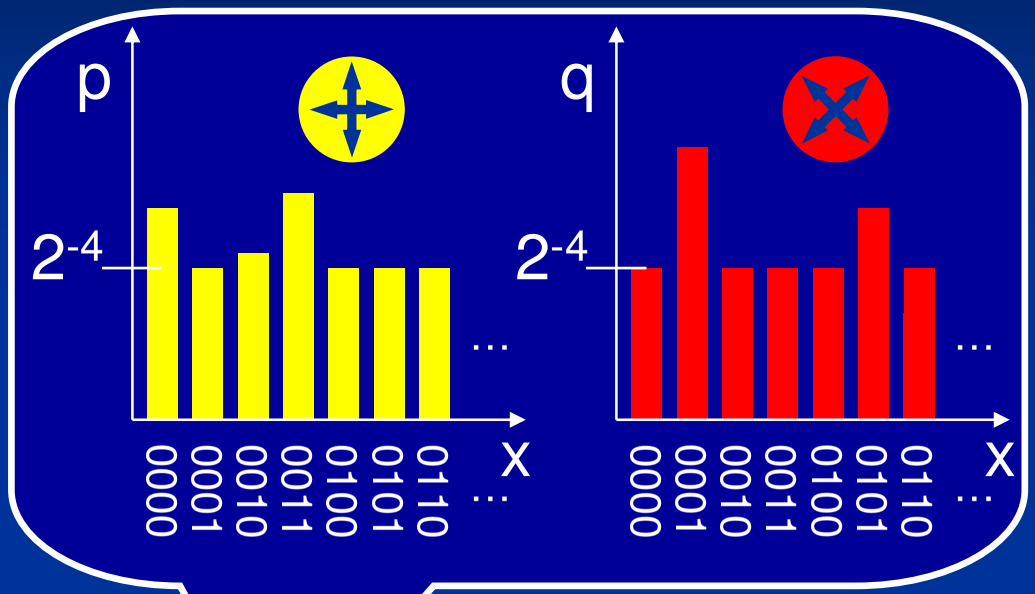
$s = b \oplus h(x)$

r, h, s

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

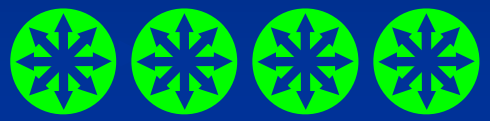
Proof of Obliviousness: Distributions II

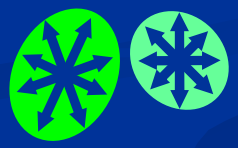
Alice



Bob

store all qubits!

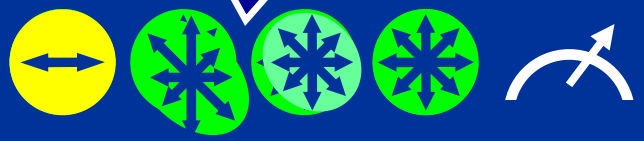




001…

memory bound: store < n/2 qubits

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



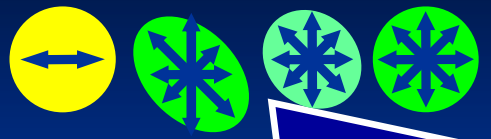
$h \in_R H_n$

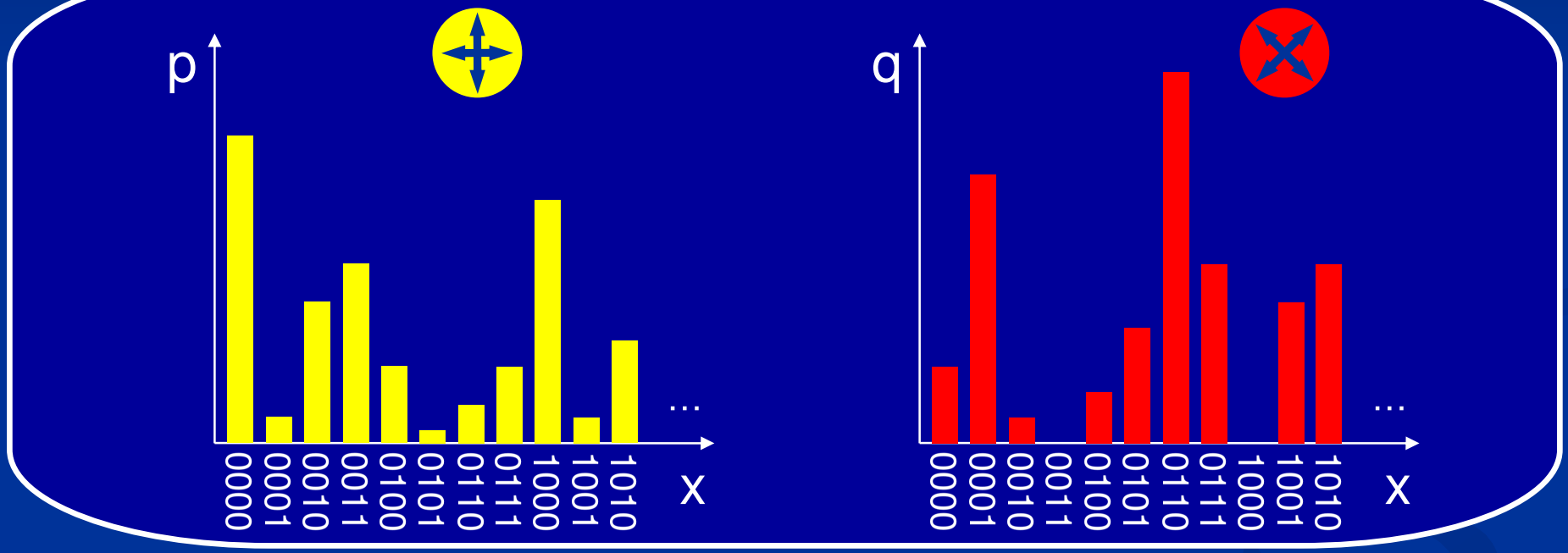
$s = b \oplus h(x)$

r, h, s

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

Proof of Sender-Privacy: Goal



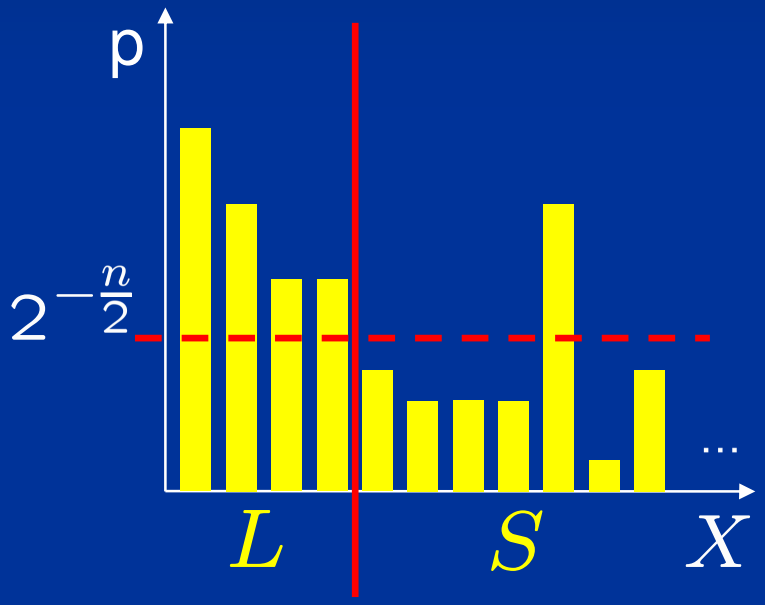


However Bob prepares his memory 001…

and the distributions p and q, he cannot guess h(x) in **both bases simultaneously** $\Rightarrow$ **sender-private**

Privacy Amplification

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

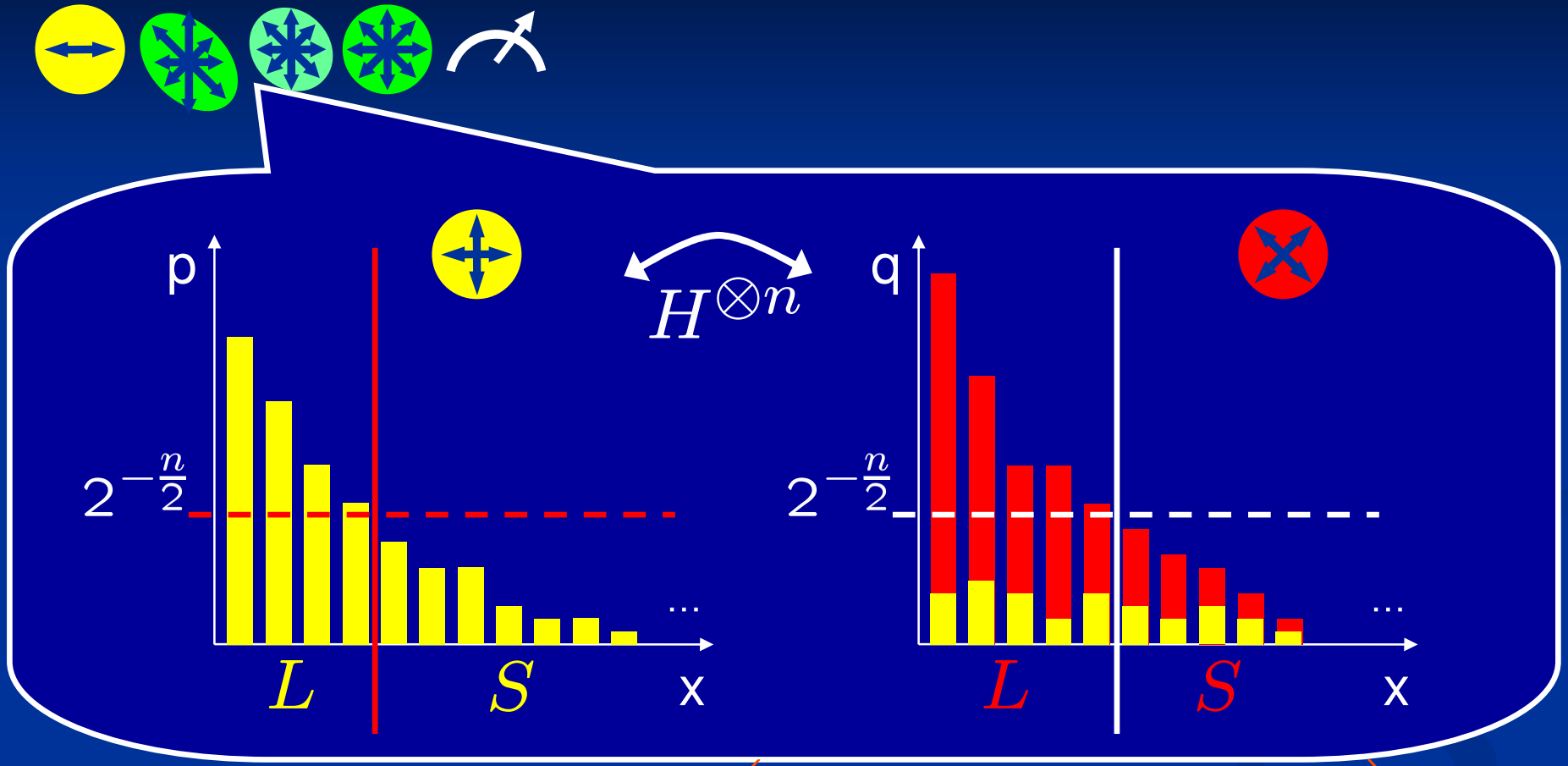


$$x \in S$$
$$\Rightarrow h(x) = ???$$

Theorem: $d(h(X)|h \otimes \boldsymbol{\rho}) \leq 2^{-\frac{1}{2}(H_\infty(\{X\}\otimes\boldsymbol{\rho})-H_0(\boldsymbol{\rho})-1)}$

$$\leq 2^{-\frac{1}{2}(H_\infty(X)-n/2-1)}$$

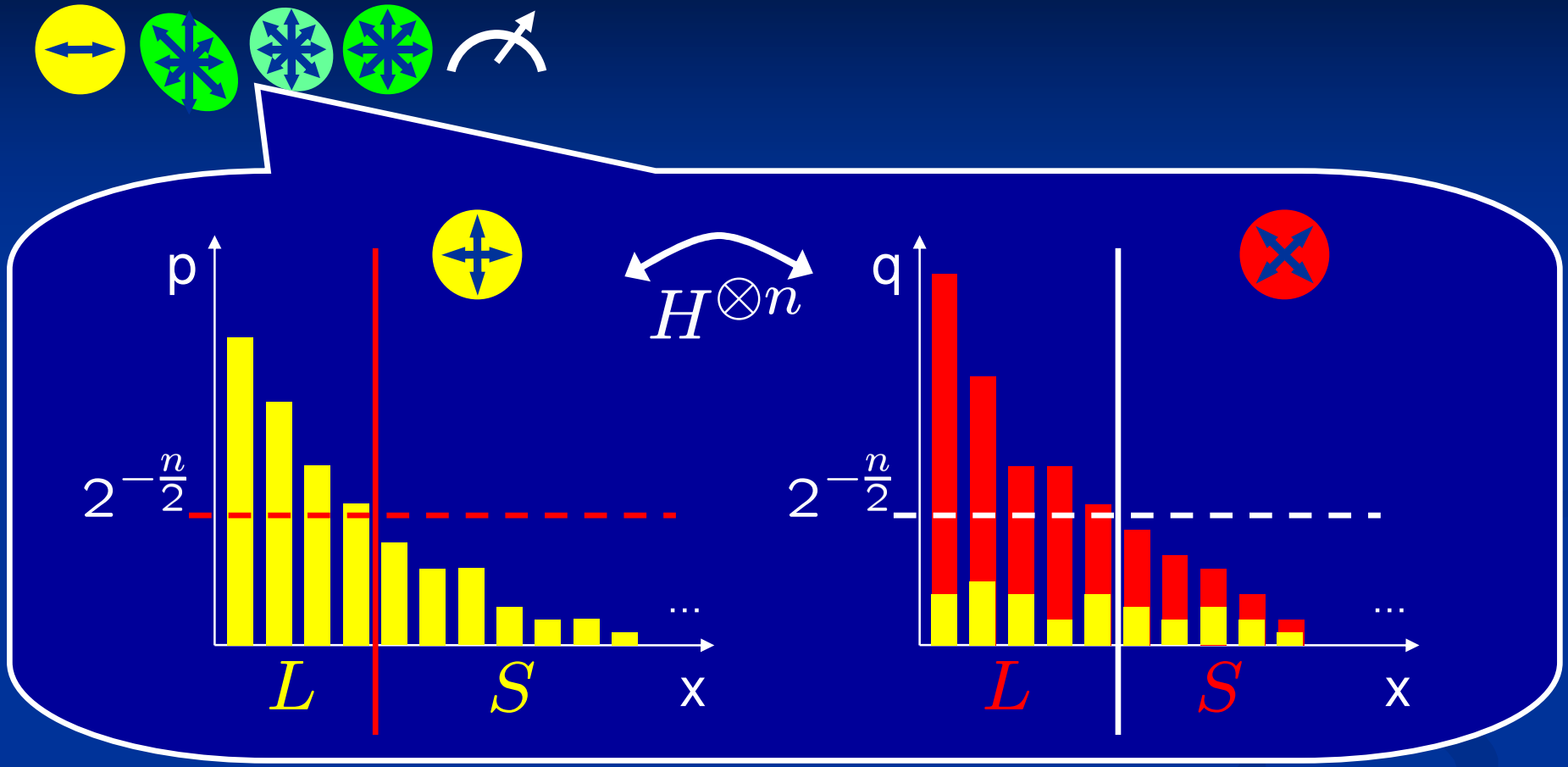
Sender-Privacy: Transformation



$$H^{\otimes n} \sum_{x \in L} \sqrt{p_x} |x\rangle = \sum_z \left(2^{-n/2} \sum_{x \in L} \sqrt{p_x} (-1)^{x \cdot z} \right) |z\rangle$$

$$|L| \leq 2^{n/2}$$

Sender-Privacy: Uncertainty Relation



$$p(S) + negl(n) \geq q(L) = 1 - q(S)$$

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

General Uncertainty Relation

n-qubit register ρ

p q $L^+, L^\times \subset \{0,1\}^n$

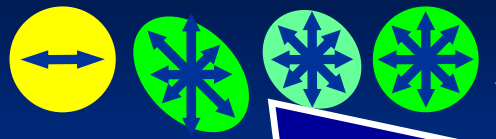
Theorem:

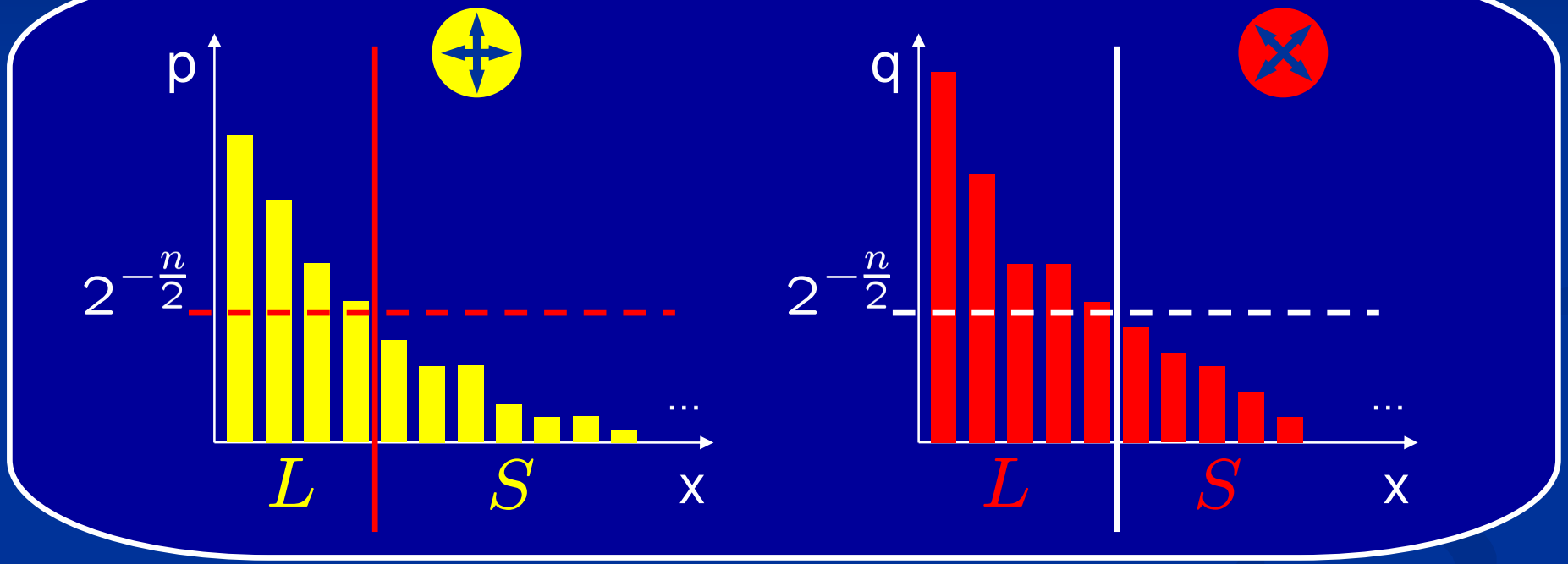
$$p(L^+) + q(L^\times) \leq \left(1 + \sqrt{2^{-n}|L^+||L^\times|}\right)^2$$

can be generalised to more than two mutually unbiased bases

Corollary: $p(S) + q(S) \geq 1 - negl(n)$

Proof of Sender-Privacy: Finale





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

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

Proof of Sender-Privacy: Recap

Alice

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

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

Bob

store all qubits!

memory bound: store < n/2 qubits

$h \in_R H_n$

$s = b \oplus h(x)$

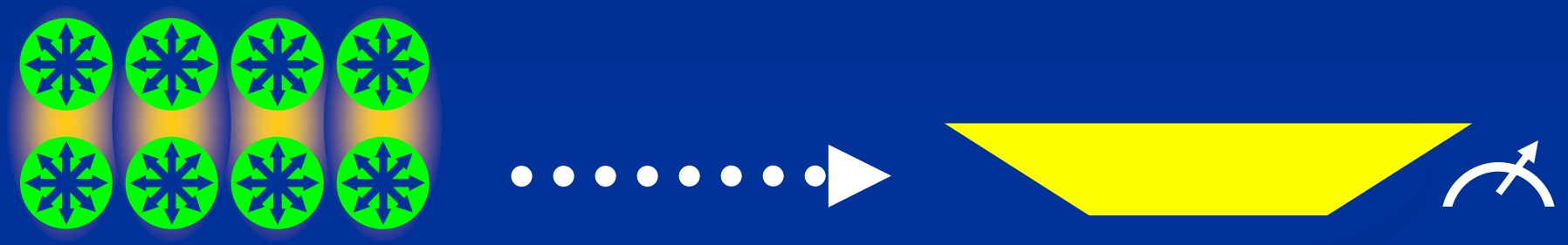
r, h, s

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

Proof of Sender-Privacy: Recap II

Alice **Bob**

store all qubits!



memory bound: store < n/2 qubits

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

$h \in_R H_n$

$s = b \oplus h(x)$

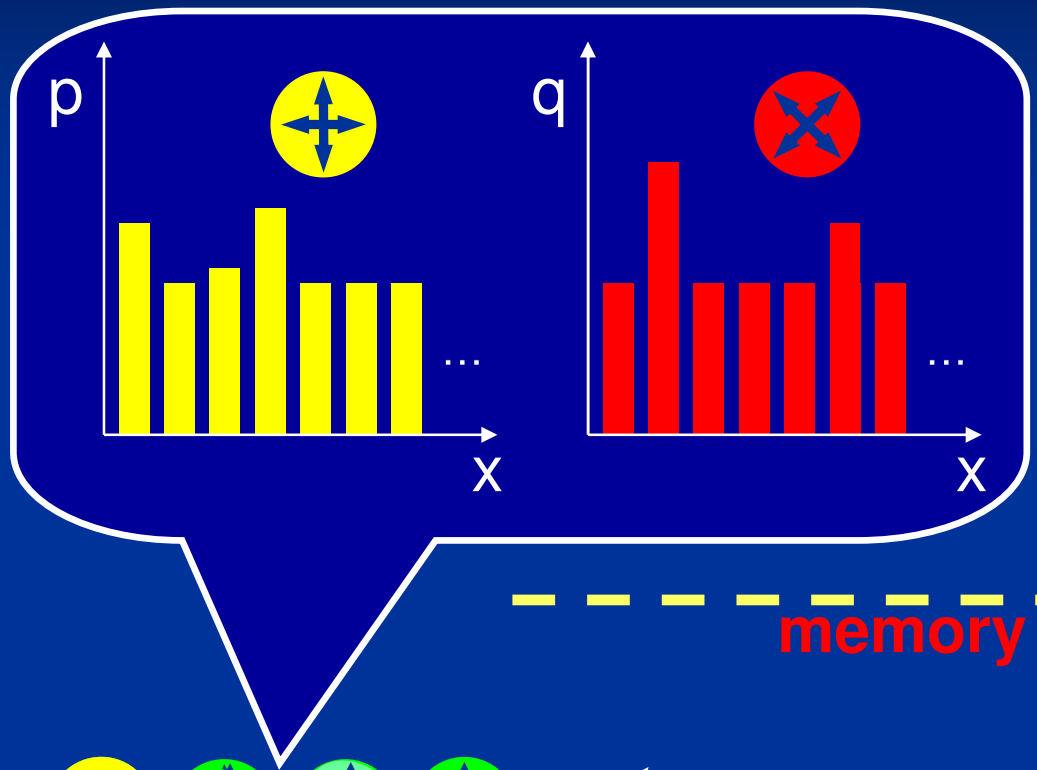
r, h, s

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

if $r = r'$

Proof of Sender-Privacy: Recap III

Alice



Bob

store all qubits!

001…

memory bound: store < n/2 qubits

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

$h \in_R H_n$

$s = b \oplus h(x)$

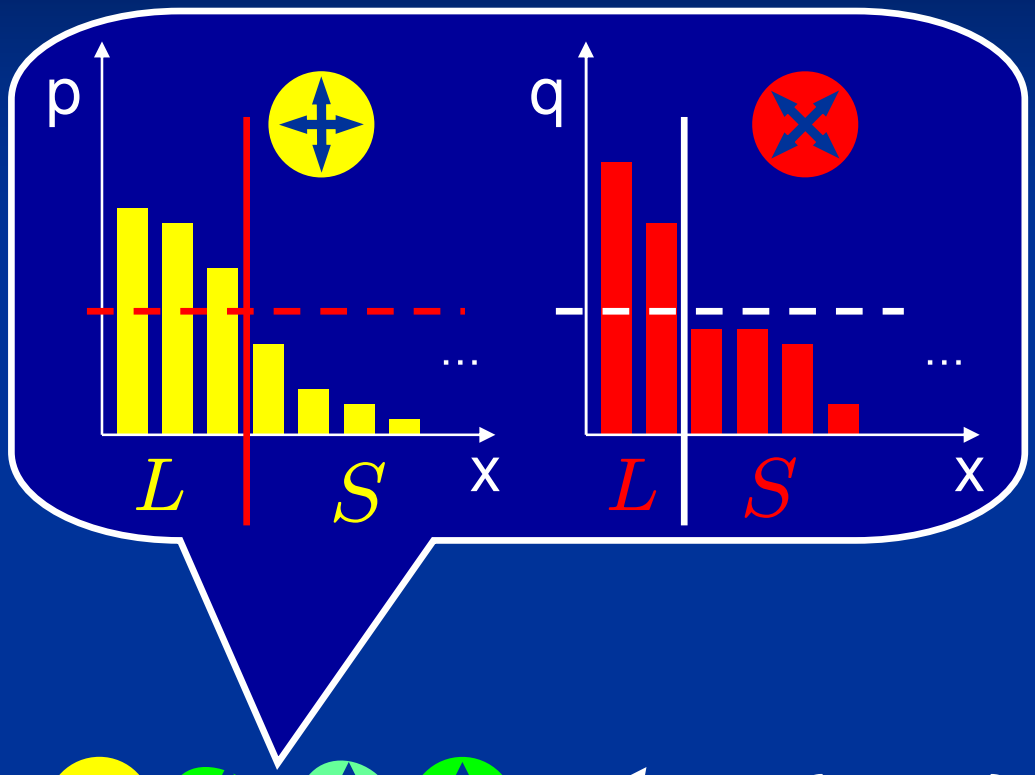
r, h, s

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

if $r = r'$

Proof of Sender-Privacy: Recap IV

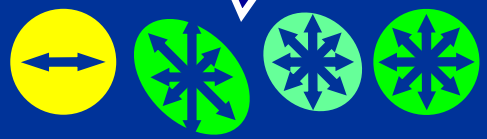
Alice



Bob

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

□



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

$h \in_R H_n$

$s = b \oplus h(x)$

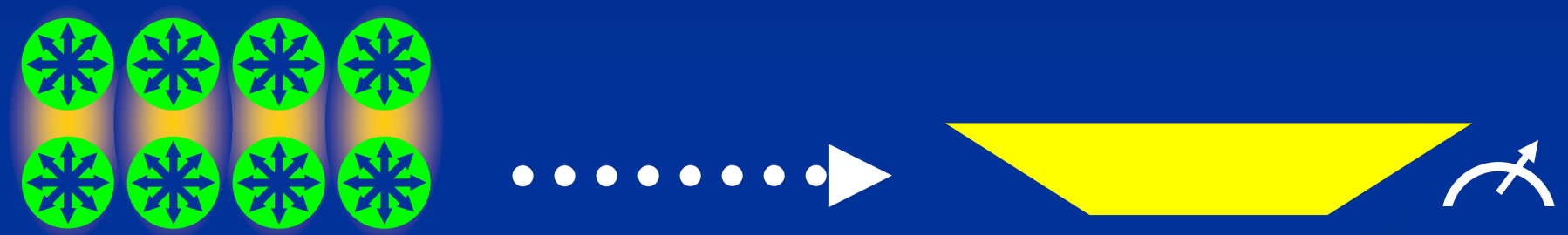
r, h, s

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

Privacy Amplification is Necessary

Alice **Bob**

store all qubits!



memory bound: store < n/2 qubits

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

$h \in_R H$ $x = x_1 \oplus x_2 \oplus \ldots$

$s = b \oplus h(x)$

r, h, s

$y' = x'_1 \oplus x'_2 \oplus \ldots$

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

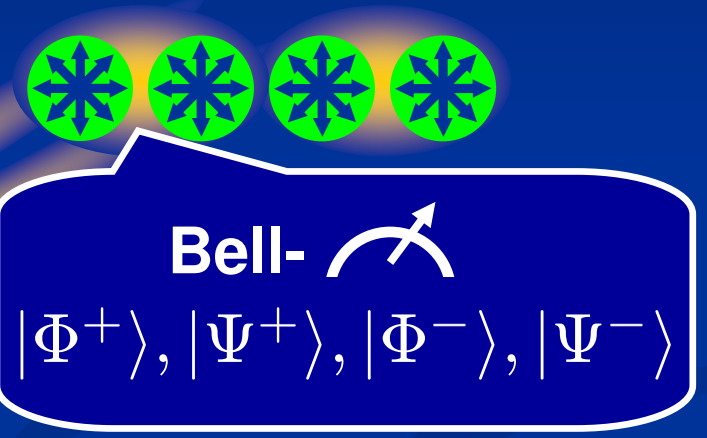
if $r = r'$ gets $b = s \oplus y'$

Privacy Amplification is Necessary II

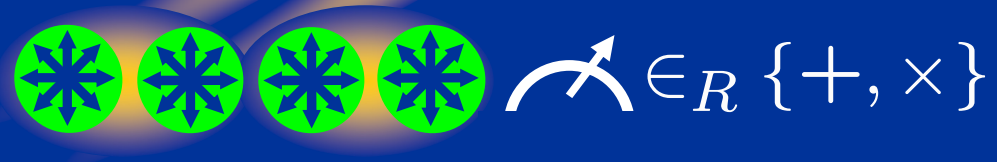
Alice

Bob

$$|\Phi^+\rangle = |00\rangle_+ + |11\rangle_+ = |00\rangle_\times + |11\rangle_\times$$
$$|\Psi^+\rangle = |01\rangle_+ + |10\rangle_+ = |00\rangle_\times - |11\rangle_\times$$
$$|\Phi^-\rangle = |00\rangle_+ - |11\rangle_+ = |01\rangle_\times + |10\rangle_\times$$
$$|\Psi^-\rangle = |01\rangle_+ - |10\rangle_+ = |10\rangle_\times - |01\rangle_\times$$



memory bound: store < n/2 qubits



$y = x_1 \oplus x_2 \oplus \ldots$

$s = b \oplus y$

r, s

$y' = x'_1 \oplus x'_2 \oplus \ldots$

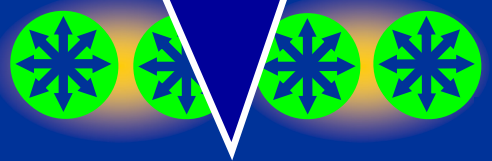
gets $b = s \oplus y'$

Privacy Amplification is Necessary !

Alice

$$|\Phi^+\rangle = |00\rangle_+ + |11\rangle_+ = |00\rangle_\times + |11\rangle_\times$$
$$|\Psi^+\rangle = |01\rangle_+ + |10\rangle_+ = |00\rangle_\times - |11\rangle_\times$$
$$|\Phi^-\rangle = |00\rangle_+ - |11\rangle_+ = |01\rangle_\times + |10\rangle_\times$$
$$|\Psi^-\rangle = |01\rangle_+ - |10\rangle_+ = |10\rangle_\times - |01\rangle_\times$$

$= 1$ if $r = +$
$= 0$ if $r = \times$



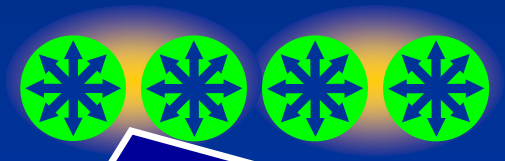
$\in_R \{+, \times\}$

$y = x_1 \oplus x_2 \oplus \ldots$

$s = b \oplus y$

r, s

Bob



Bell- 

$|\Psi^+\rangle$

memory bound: store < n/2 qubits

storing ≤ 1 qubit,
Bob learns y and
gets $b' = s \oplus y \oplus \ldots$
all the time!

Agenda

- ✓ Two-Party Crypto Primitives
- ✓ Protocol for Oblivious Transfer
- ✓ Security Proof
- **Protocol for Bit Commitment**
- Practicality Issues
- Open Problems

Quantum Protocol for Bit Commitment

Verifier

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

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

Committer

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

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

obtains x' by measuring all qubits in basis b

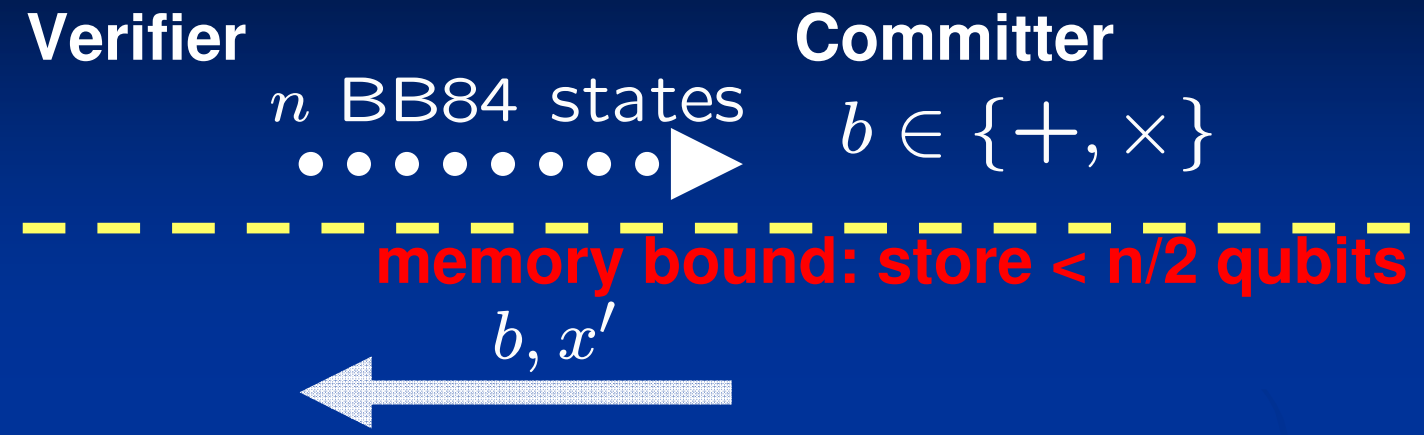
BC

memory bound: store < n/2 qubits

b, x' ◀

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

Quantum Protocol for Bit Commitment II



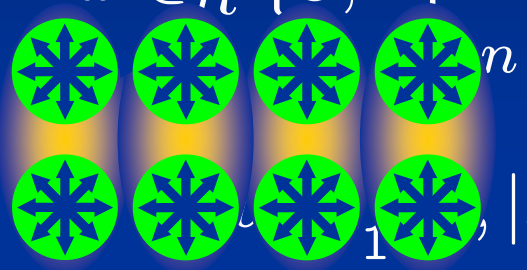
BC

- one round, non-interactive
- commit by receiving!
  application: e.g. passive time-stamping
- 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**

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



$|x_1\rangle_{r_1}, \ldots, |x_n\rangle_{r_n}$

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

- ✓ Two-Party Crypto Primitives
- ✓ Protocol for Oblivious Transfer
- ✓ Security Proof
- ✓ Protocol for Bit Commitment
- **Practicality Issues**
- Open Problems

Practicality Issues

OT

- Use polarization of photons as quantum states
- state-of-the-art technology
  - **can** transmit (encode, send over fibers, receive and measure) quantum bits
  - **cannot store** them for longer than a few milliseconds

BC

Problems:

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

Practicality Issues II

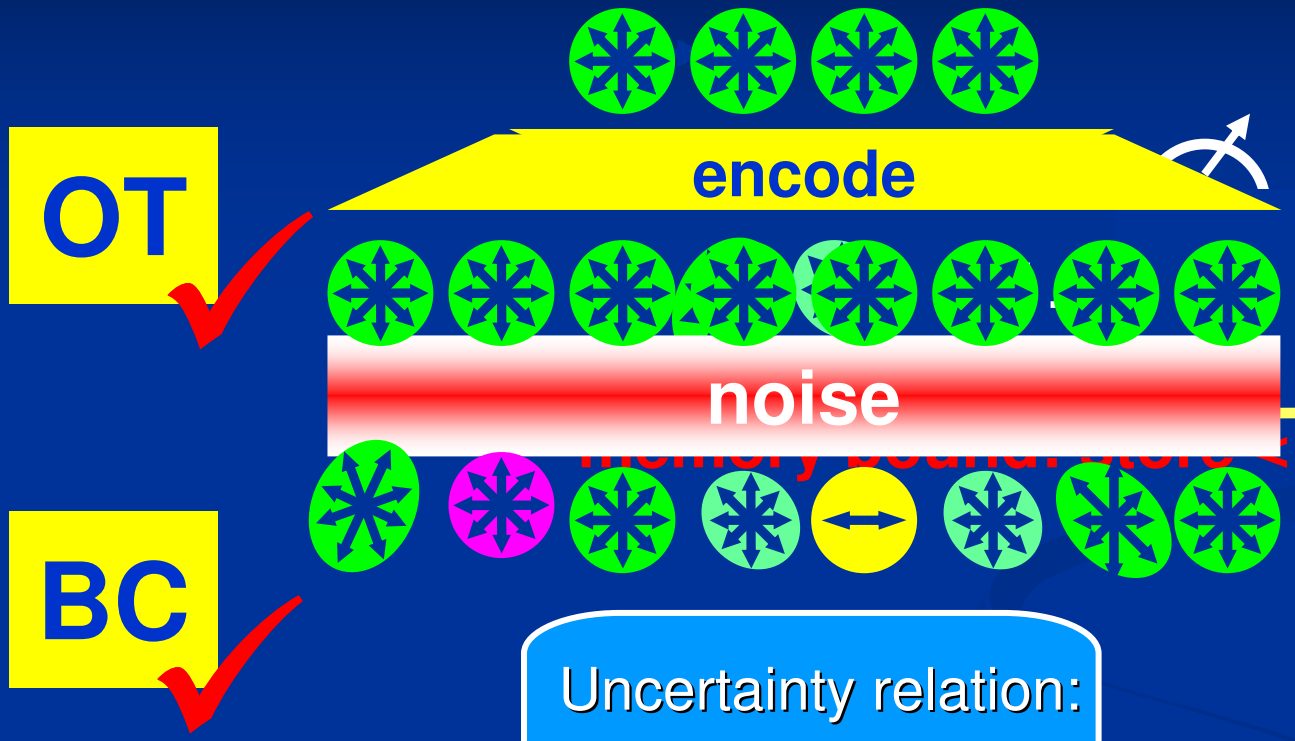
Our protocols can be modified to

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

➔ Well within reach of **current technology**

➔ **unconditionally secure** as long as nobody can store large amounts of quantum bits

More Realistic: Noisy Memory Models



$\geq n$ qubits

memory bound: store $< n/2$ qubits

random state ρ with $H_0(\rho) < n/2$

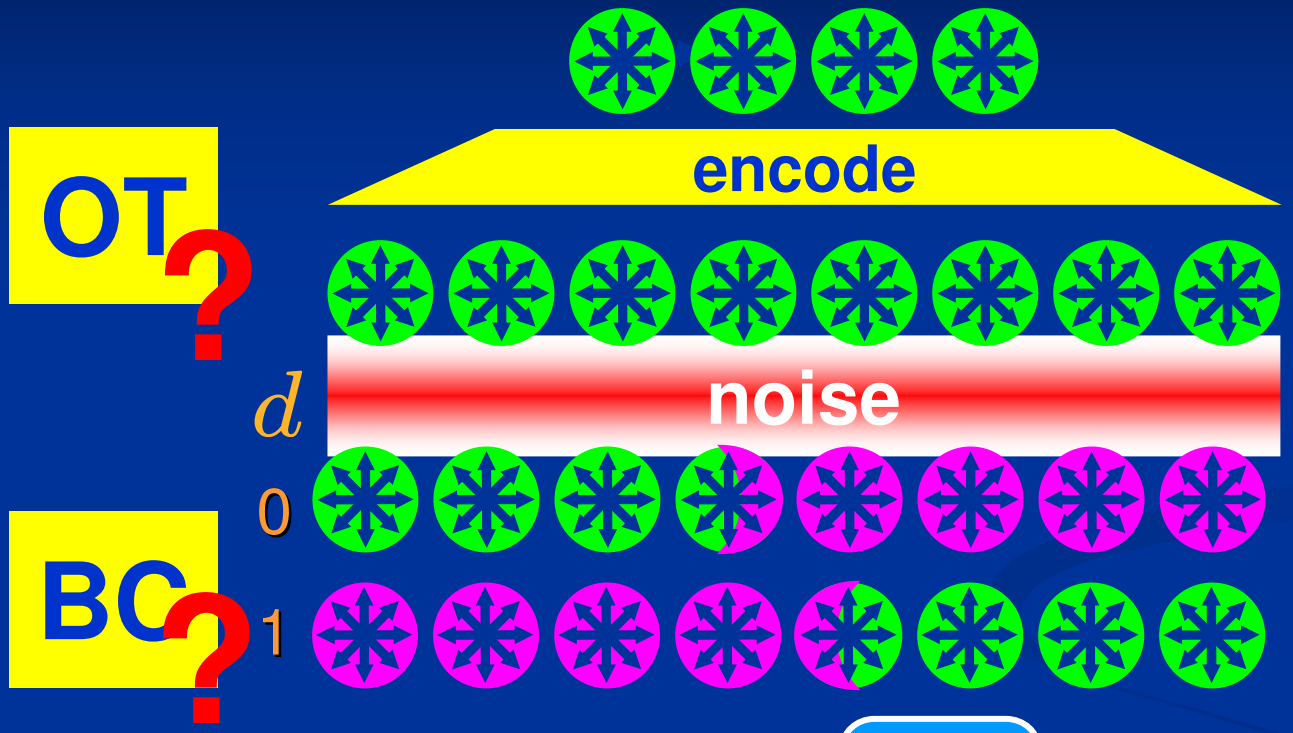
Uncertainty relation: $\geq n/2$, given $\mathcal{E}$

$= \log(\mathrm{rank}(\rho)) < n/2$

Privacy Amplification:

$$d(h(X)|h \otimes \rho) \leq 2^{-\frac{1}{2}(H_\infty(\{X\}\otimes\rho) - H_0(\rho) - 1)}$$

Open Problem: Noisy Memory Models



$\geq n$ qubits

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

given d, a random state ρ with $H_0(\rho) \leq n/2$

?

$= \log(\mathrm{rank}(\rho)) < n/2$

Privacy Amplification:

$$d(h(X)|h \otimes \rho) \leq 2^{-\frac{1}{2}(H_\infty(\{X\} \otimes \rho) - H_0(\rho) - 1)}$$

Open Problems and Next Steps

- Noisy Memory Model
- Other flavors of OT:
  e.g. 1-out-of-2 Oblivious Transfer
- Better memory bounds
- Composability? What happens to the memory bound?
- Cryptographic primitives for which we can show lower bounds

Summary

Simple 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
  - work in more practical noisy memory models

Quantum Protocol for 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

r, h_0, h_1 ⟶

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

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

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

s_0, s_1 ⟶

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

Questions and Comments?

OT

BC