

# **Introduction to Quantum Information Processing**

## **Lecture 17**

**Richard Cleve**

# Overview of Lecture 17

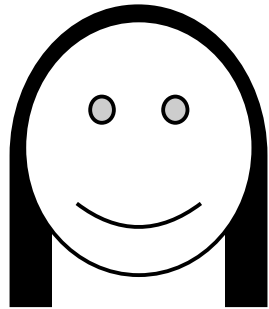
- Introduction to **communication complexity**
- Intersection problem (a.k.a. appointment scheduling)
- Restricted equality problem
- Exponential separation in bounded-error setting
- Inner product problem
- Simultaneous message passing model and fingerprinting

**communication  
complexity**

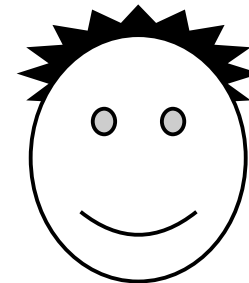
# Classical communication complexity

[Yao, 1979]

$x_1 x_2 \dots x_n$



$y_1 y_2 \dots y_n$



$f(x, y)$

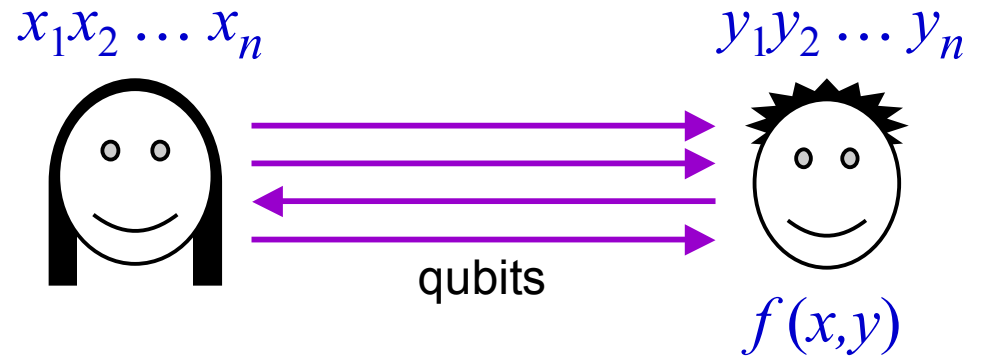
E.g. equality function:  $f(x, y) = 1$  if  $x = y$ , and  $0$  if  $x \neq y$

Any **deterministic** protocol requires  $n$  bits communication

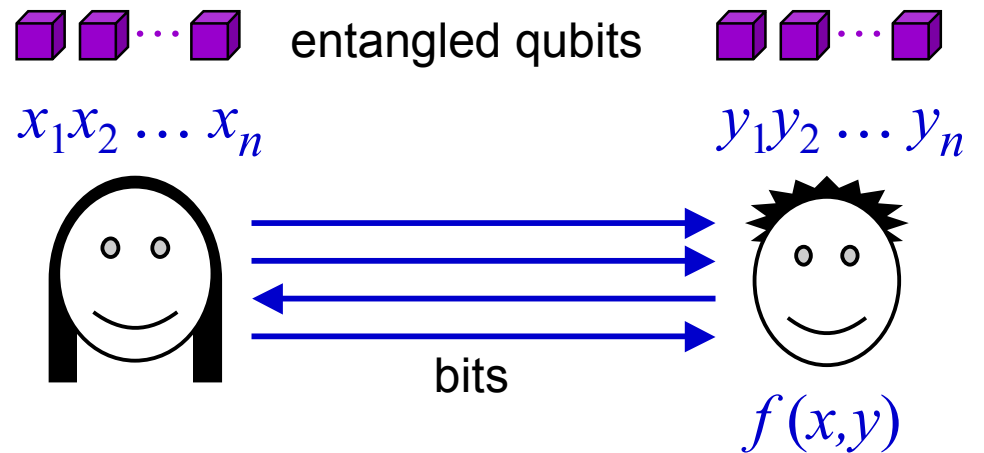
**Probabilistic** protocols can solve with only  $O(\log(n/\epsilon))$  bits communication (error probability  $\epsilon$ ), **via random hashing**

# Quantum communication complexity

Qubit communication



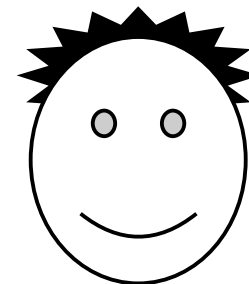
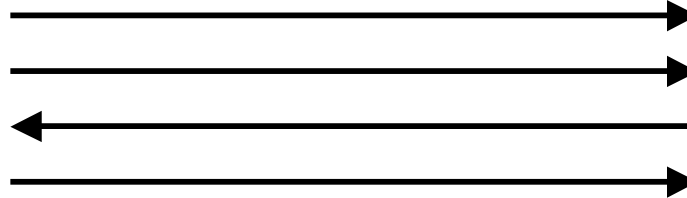
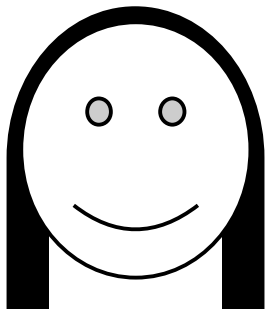
Prior entanglement



# Appointment scheduling

$$x = \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & \dots & n \\ \hline 0 & 1 & 1 & 0 & 1 & \dots & 0 \end{array}$$

$$y = \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & \dots & n \\ \hline 1 & 0 & 0 & 1 & 1 & \dots & 1 \end{array}$$



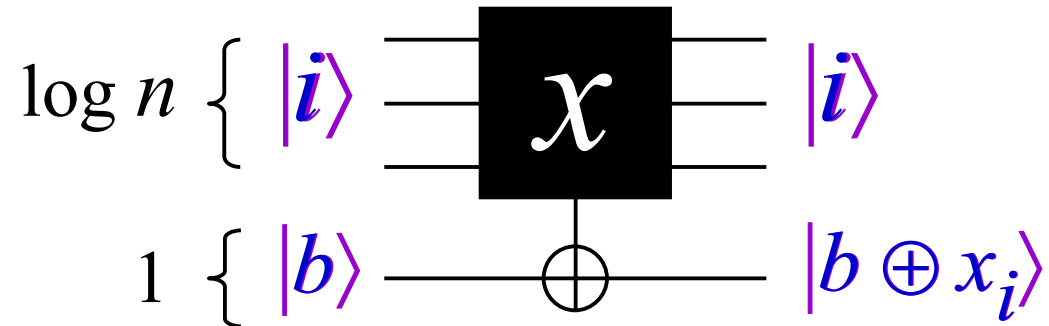
$$i \quad (x_i = y_i = 1)$$

Classically,  $\Omega(n)$  **bits** necessary to succeed with prob.  $\geq 3/4$

For all  $\varepsilon > 0$ ,  $O(n^{1/2} \log n)$  **qubits** sufficient for error prob.  $< \varepsilon$

# Search problem

Given:  $x = \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & \dots & n \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & \dots & 1 \end{array}$  accessible via *queries*



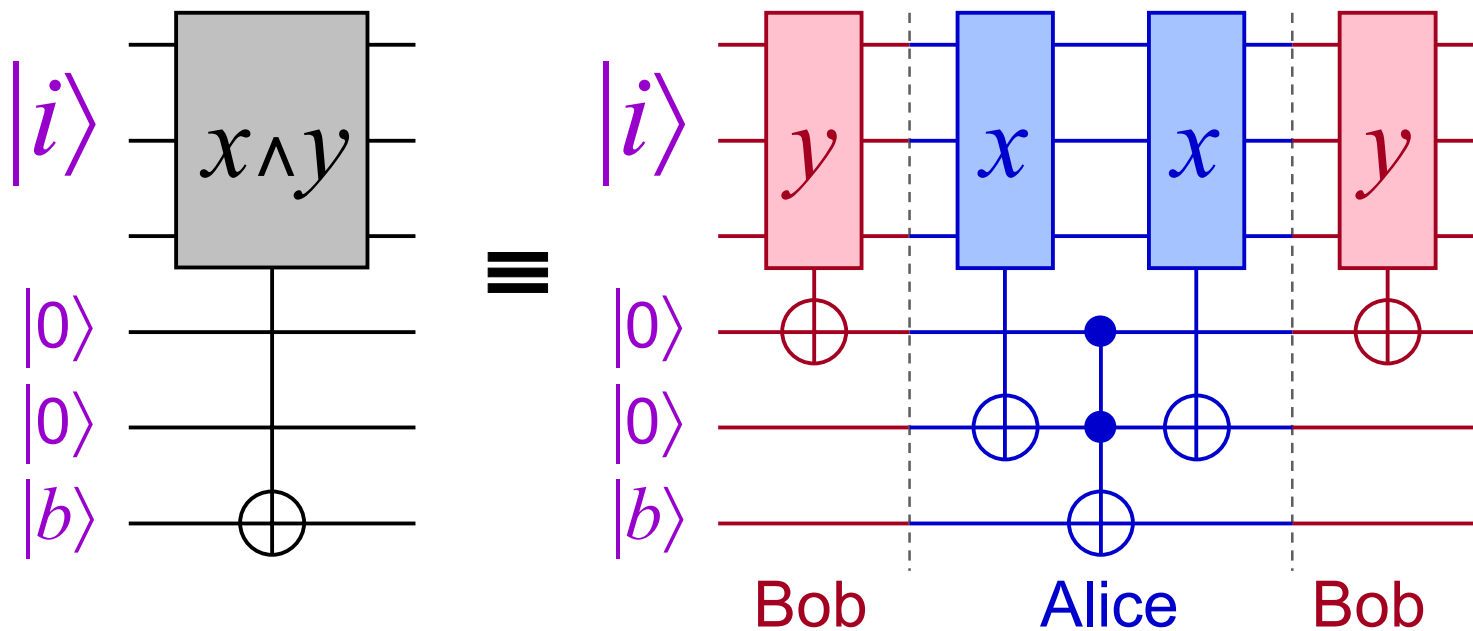
**Goal:** find  $i \in \{1, 2, \dots, n\}$  such that  $x_i = 1$

**Classically:**  $\Omega(n)$  queries are necessary

**Quantum mechanically:**  $O(n^{1/2})$  queries are sufficient

[Grover, 1996]

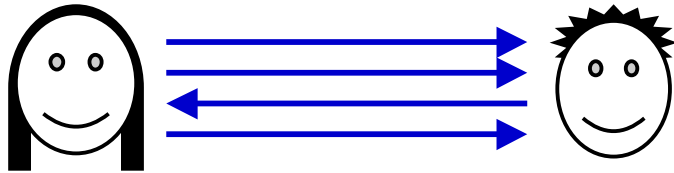
		1	2	3	4	5	6	...	$n$
Alice	$x =$	0	1	1	0	1	0	...	0
Bob	$y =$	1	0	0	1	1	0	...	1
	$x \wedge y =$	0	0	0	0	1	0	...	0



Communication per  $x \wedge y$ -query:  $2(\log n + 3) = O(\log n)$

# Appointment scheduling: epilogue

Bit communication:



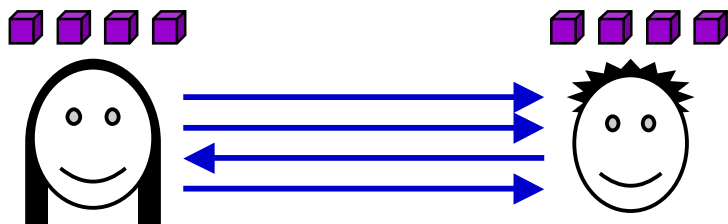
Cost:  $\theta(n)$

Qubit communication:



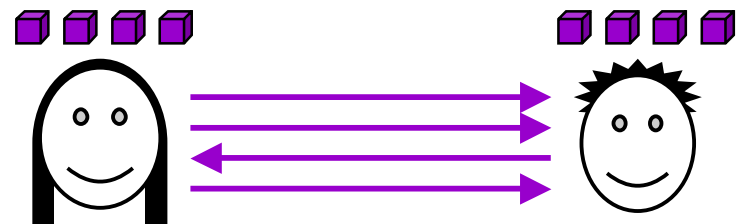
Cost:  $\theta(n^{1/2})$  (with refinements)

Bit communication  
& prior entanglement:



Cost:  $\theta(n^{1/2})$

Qubit communication  
& prior entanglement:



Cost:  $\theta(n^{1/2})$

# Restricted version of equality

Precondition (i.e. promise): either  $x = y$  or  $\Delta(x,y) = n/2$   
Hamming distance

(Distributed variant of “constant” vs. “balanced”)

Classically,  $\Omega(n)$  bits communication are necessary  
**for an exact solution**

Quantum mechanically,  $O(\log n)$  qubits communication  
are sufficient **for an exact solution**

# Classical lower bound

**Theorem:** If  $S \subseteq \{0,1\}^n$  has the property that, for all  $x, x' \in S$ , their *intersection* size is *not*  $n/4$  then  $|S| < 1.99^n$

Let **some** protocol solve restricted equality with  $k$  bits comm.

- $2^k$  conversations of length  $k$
- approximately  $2^n/\sqrt{n}$  input pairs  $(x, x)$ , where  $\Delta(x) = n/2$

Therefore,  $2^n/2^k\sqrt{n}$  input pairs  $(x, x)$  that yield **same** conv.  $C$

Define  $S = \{x : \Delta(x) = n/2 \text{ and } (x, x) \text{ yields conv. } C\}$

For any  $x, x' \in S$ , input pair  $(x, x')$  **also** yields conversation  $C$

Therefore,  $\Delta(x, x') \neq n/2$ , implying intersection size is **not**  $n/4$

Theorem implies  $2^n/2^k\sqrt{n} < 1.99^n$ , so  $k > 0.007n$

# Quantum protocol

For each  $x \in \{0,1\}^n$ , define  $|\psi_x\rangle = \sum_{j=1}^n (-1)^{x_j} |j\rangle$

## Protocol:

1. Alice sends  $|\psi_x\rangle$  to Bob ( $\log(n)$  qubits)
2. Bob measures state in a basis that includes  $|\psi_y\rangle$

## Correctness of protocol:

If  $x = y$  then Bob's result is definitely  $|\psi_y\rangle$

If  $\Delta(x,y) = n/2$  then  $\langle \psi_x | \psi_y \rangle = 0$ , so result is definitely **not**  $|\psi_y\rangle$

---

**Question:** How much communication if error  $1/4$  is permitted?

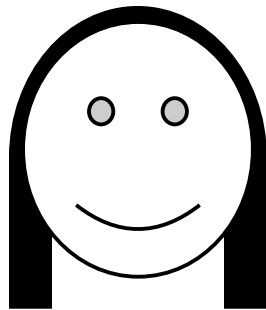
**Answer:** just 2 bits are sufficient!

# Exponential quantum vs. classical separation in bounded-error models

$O(\log n)$  quantum vs.  $\Omega(n^{1/4} / \log n)$  classical

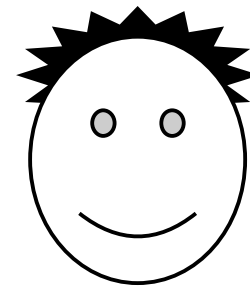
$|\psi\rangle$ : a  $\log(n)$ -qubit state  
(described *classically*)

$M$ : two-outcome measurement



**Output:** result of  
applying  $M$  to  $U|\psi\rangle$

$U$ : unitary operation  
on  $\log(n)$  qubits



# Inner product

$$\text{IP}(x, y) = x_1 y_1 + x_2 y_2 + \dots + x_n y_n \pmod{2}$$

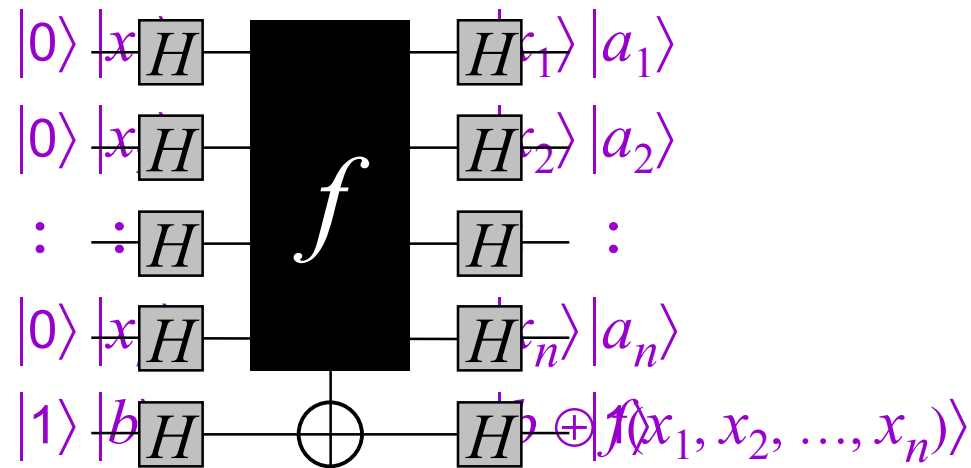
Classically,  $\Omega(n)$  bits of communication are required, even for bounded-error protocols

Quantum protocols *also* require  $\Omega(n)$  communication

# Recall the BV problem

Let  $f(x_1, x_2, \dots, x_n) = a_1 x_1 + a_2 x_2 + \dots + a_n x_n \pmod{2}$

**Given:**



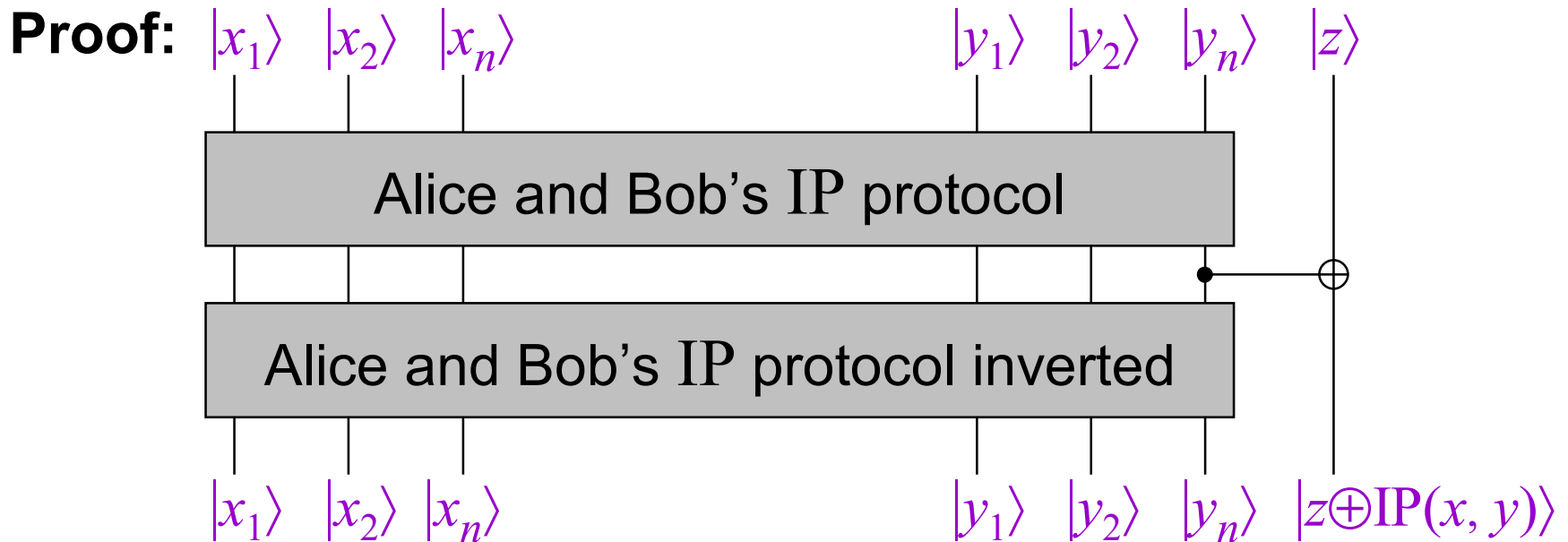
**Goal:** determine  $a_1, a_2, \dots, a_n$

Classically,  $n$  queries are necessary

Quantum mechanically, 1 query is sufficient

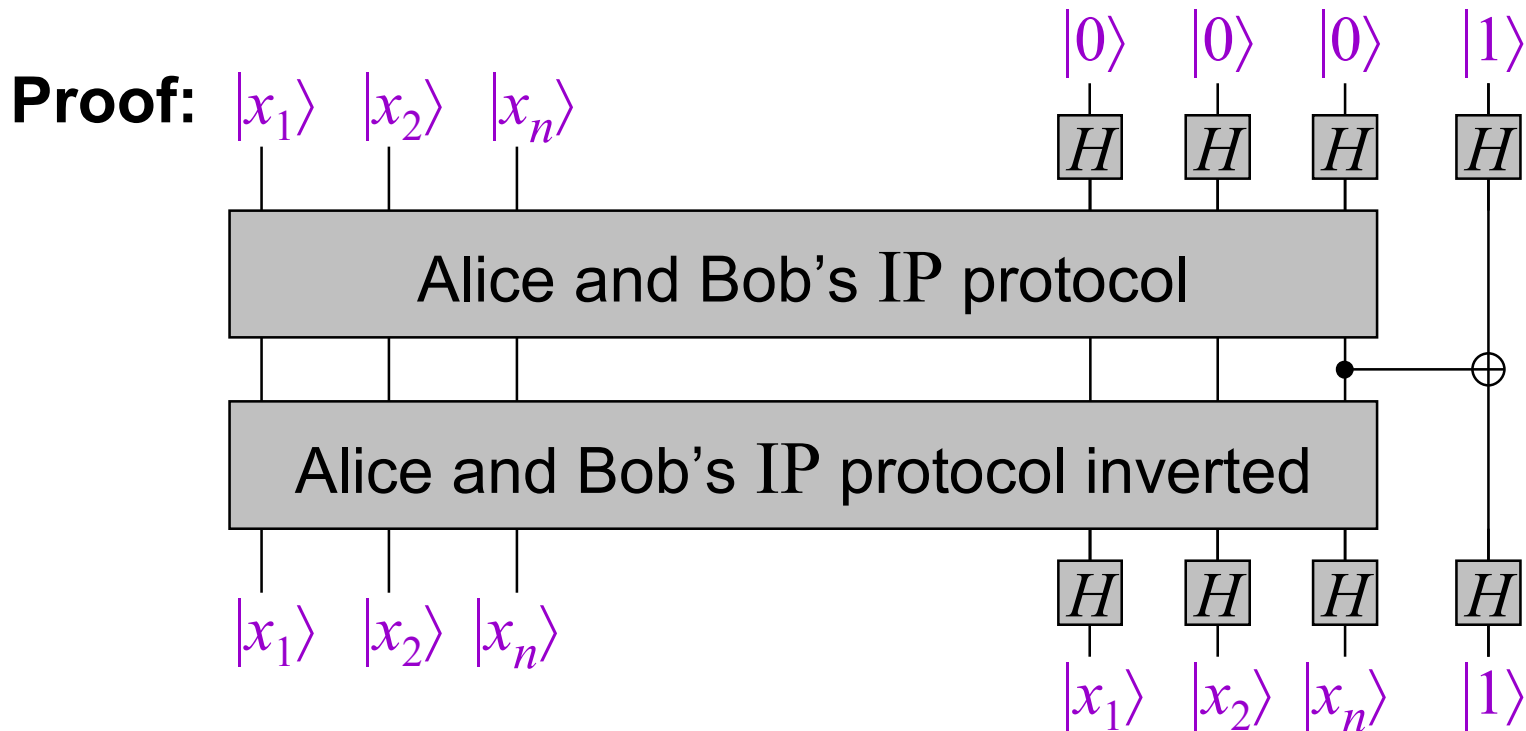
# Lower bound for inner product

$$\text{IP}(x, y) = x_1 y_1 + x_2 y_2 + \dots + x_n y_n \text{ mod } 2$$



# Lower bound for inner product

$$\text{IP}(x, y) = x_1 y_1 + x_2 y_2 + \dots + x_n y_n \text{ mod } 2$$



Since  $n$  bits are conveyed from Alice to Bob,  $n$  qubits communication necessary (by Holevo's Theorem)

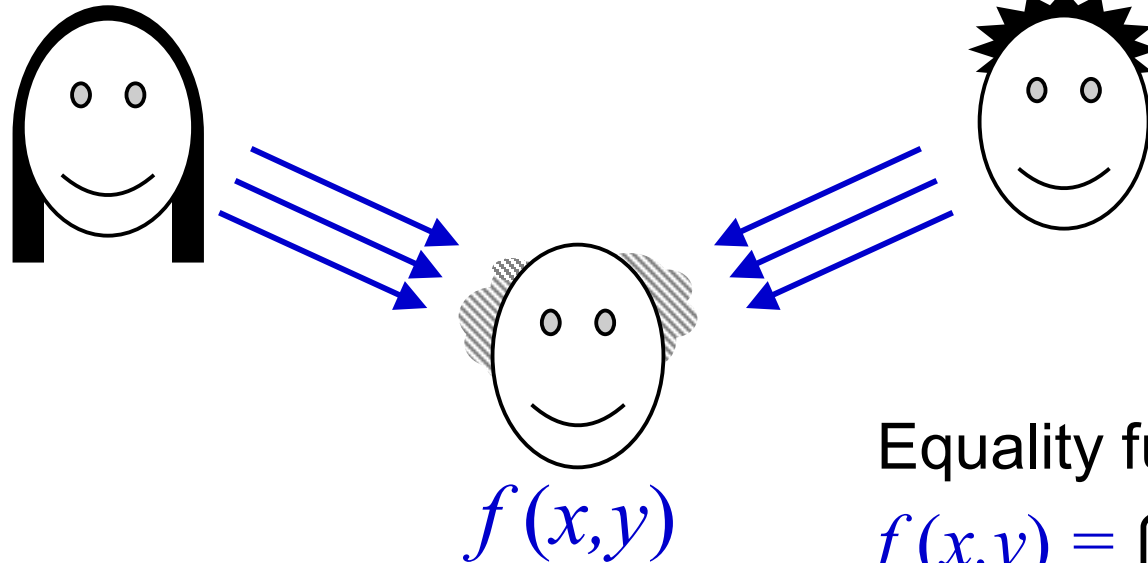
# quantum fingerprints

# Equality revisited

## in simultaneous message model

$x_1x_2 \dots x_n$

$y_1y_2 \dots y_n$



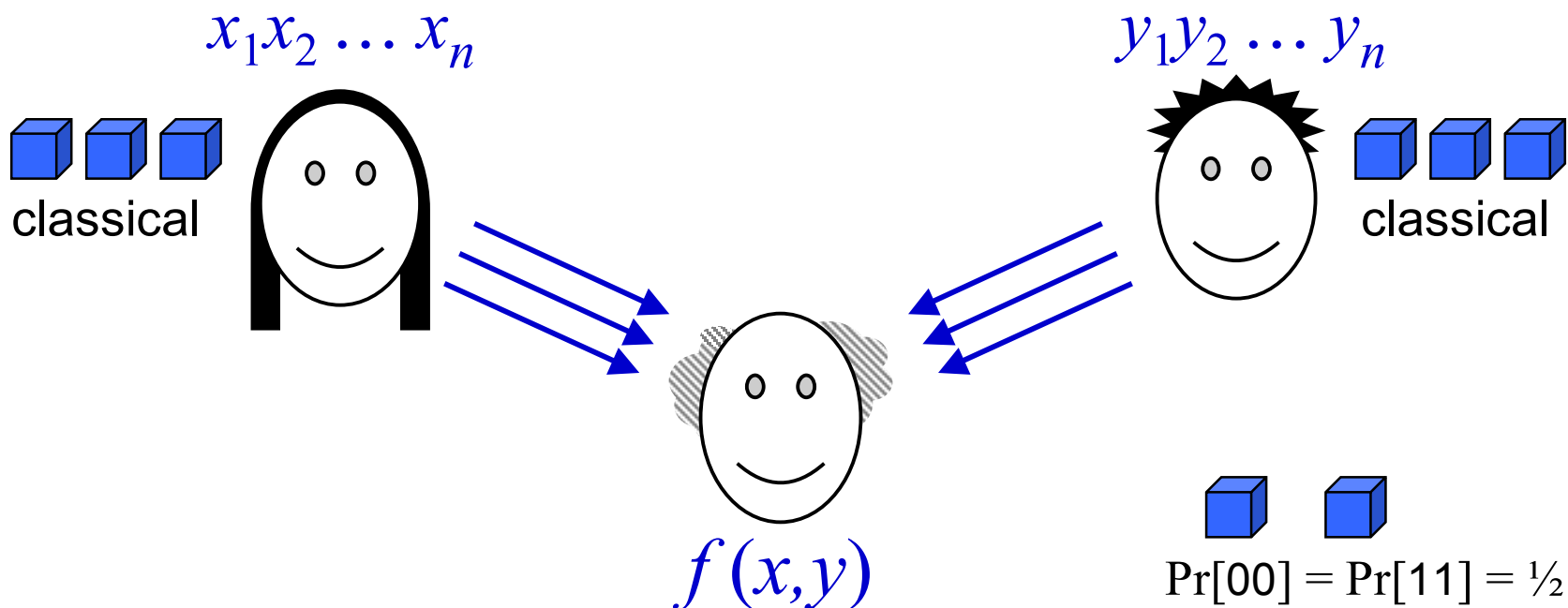
Equality function:

$$f(x,y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases}$$

**Exact protocols:** require  $2n$  bits communication

# Equality revisited

## in simultaneous message model

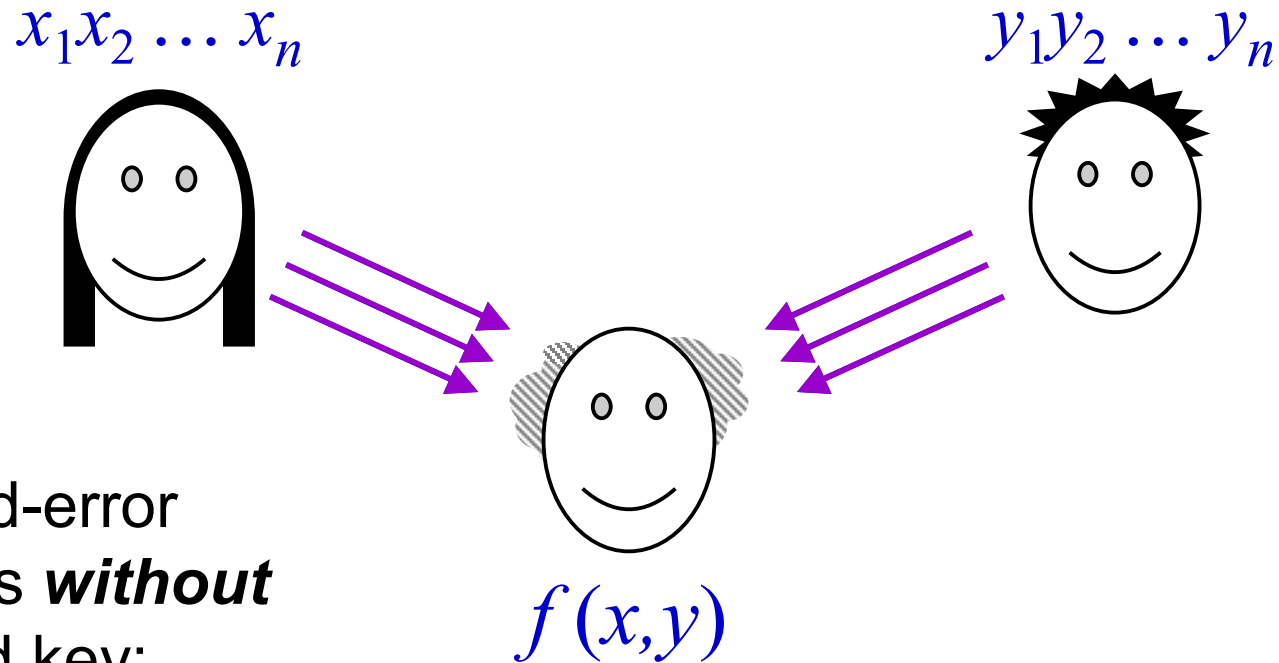


**Bounded-error protocols with a shared random key:**  
 require only  $O(1)$  bits communication

Error-correcting code:  $e(x) = 101111010110011001$   
 $e(y) = 011010010011001010$

random  $k$

# Equality revisited in simultaneous message model



Bounded-error  
protocols *without*  
a shared key:

**Classical:**  $\theta(n^{1/2})$

**Quantum:**  $\theta(\log n)$

# Quantum fingerprints

**Question 1:** how many orthogonal states in  $m$  qubits?

**Answer:**  $2^m$

Let  $\varepsilon$  be an arbitrarily small positive constant

**Question 2:** how many *almost orthogonal*\* states in  $m$  qubits?

(\* where  $|\langle \psi_x | \psi_y \rangle| \leq \varepsilon$  )

**Answer:**  $2^{2am}$ , for some constant  $a > 0$

**To be continued during next lecture ...**

**THE END**