QUANTUM INFORMATION & COMMUNICATION COMPLEXITY

RICHARD CLEVE
U OF CALGARY

1 Preliminaries

COMMUNICATION SCENARIO

GOAL IS FOR ALICE TO CONVEY **N** BITS TO BOB

$X_1, X_2, \ldots, X_N$ (BITS)

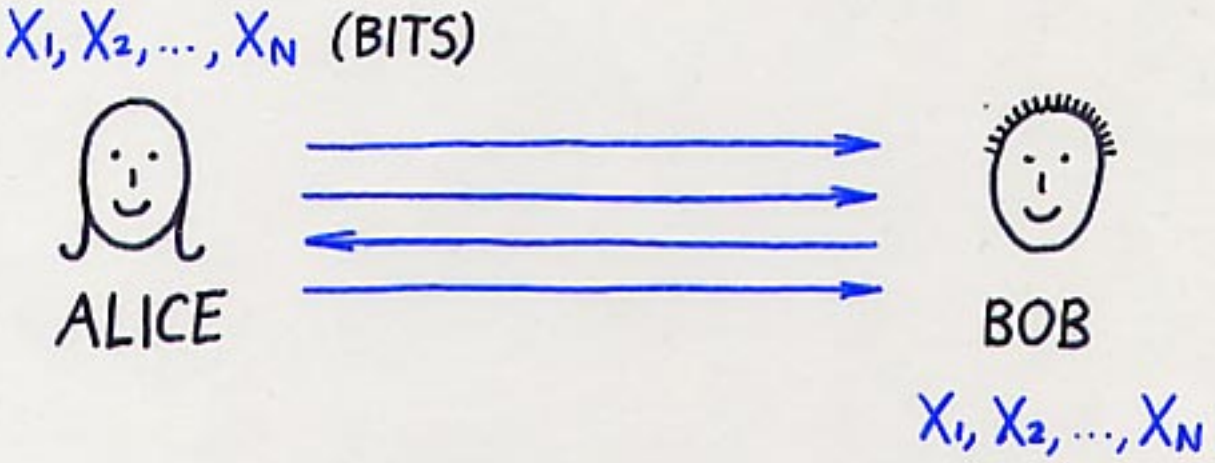
ALICE

BOB

$X_1, X_2, \ldots, X_N$

COMMUNICATION SCENARIO

GOAL IS FOR ALICE TO CONVEY **N** BITS TO BOB



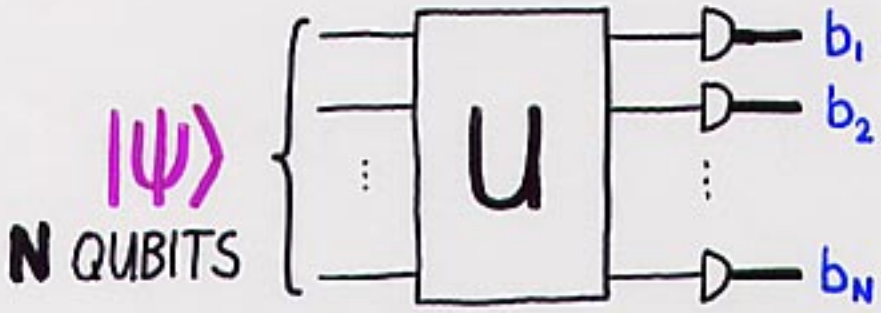
BIT COMMUNICATION: COST IS **N**

COMMUNICATION SCENARIO

GOAL IS FOR ALICE TO CONVEY **N** BITS TO BOB

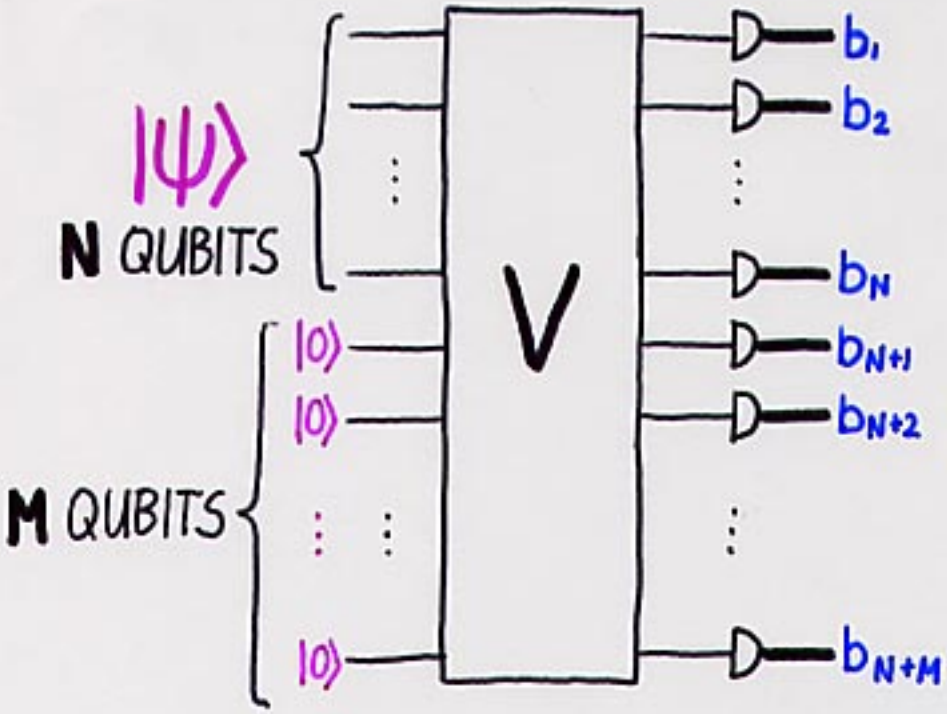
QUBIT COMMUNICATION: COST IS **N** [HOLEVO]

HOLEVO'S THEOREM-EASY CASE



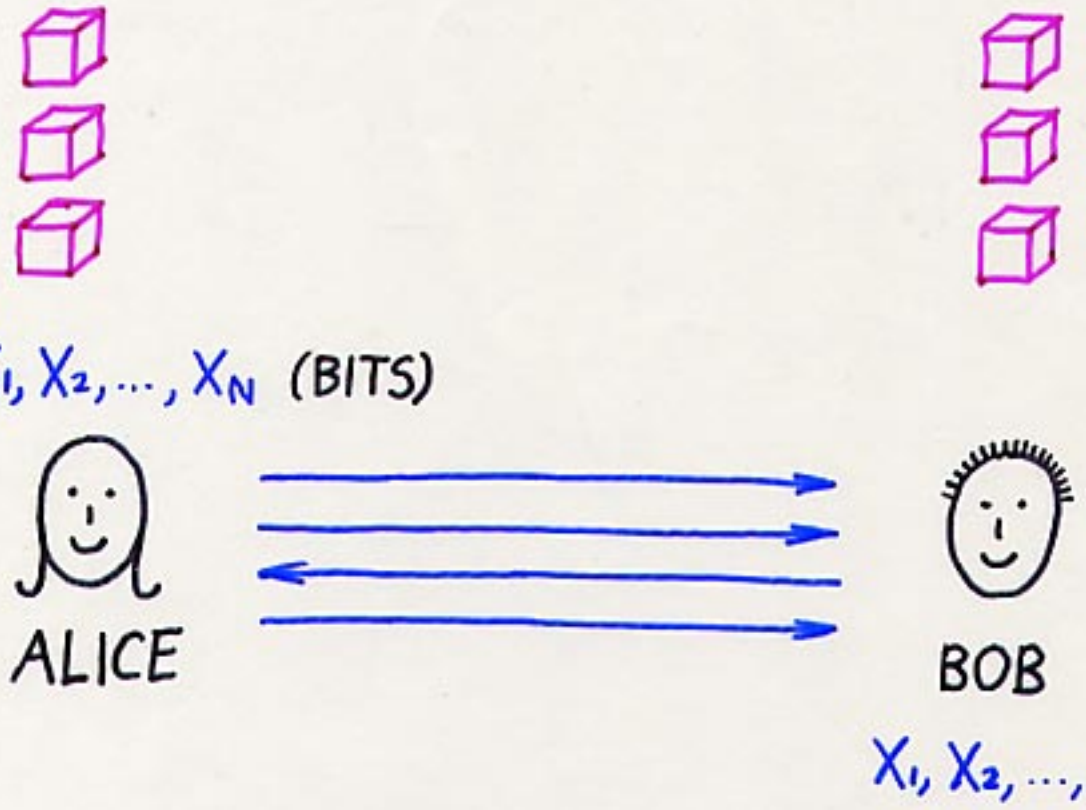
$b_1 b_2 \cdots b_N$ CANNOT CONTAIN MORE THAN **N** BITS!

HOLEVO'S THEOREM-HARD CASE



COMMUNICATION SCENARIO

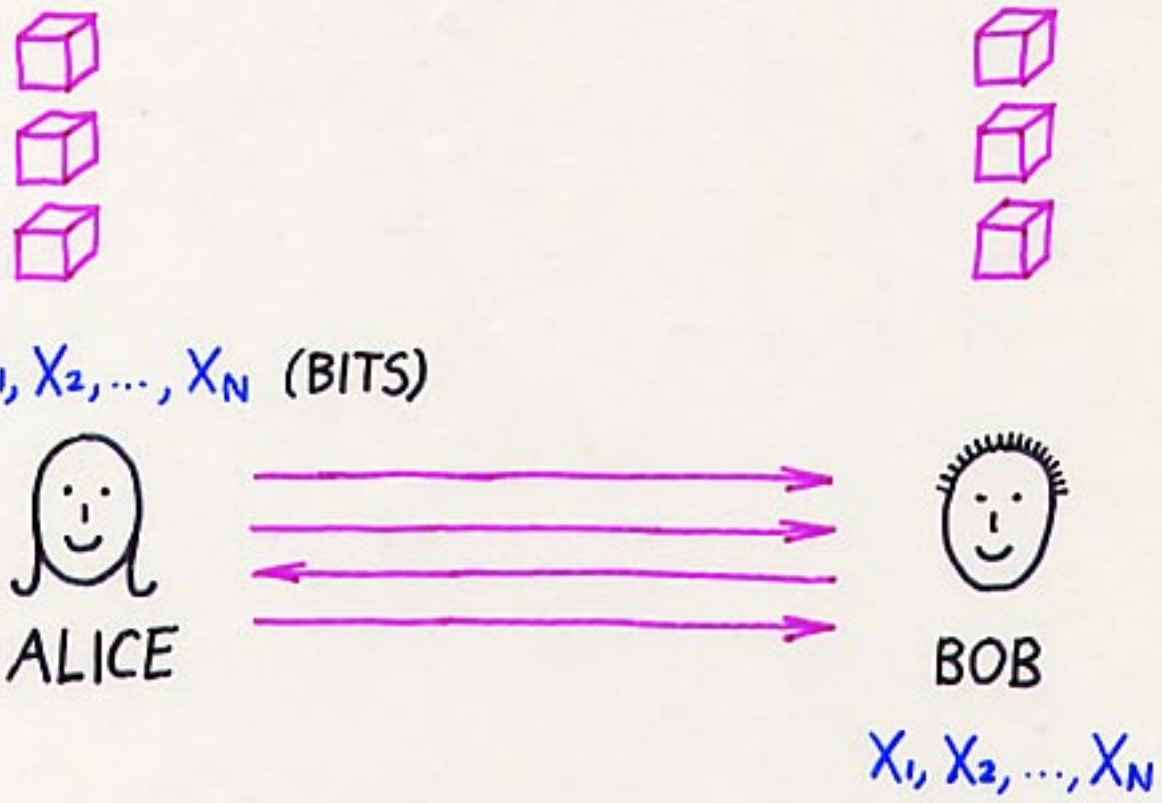
GOAL IS FOR ALICE TO CONVEY **N** BITS TO BOB



BIT COMMUNICATION WITH PRIOR ENTANGLEMENT:
COST IS **N**

COMMUNICATION SCENARIO

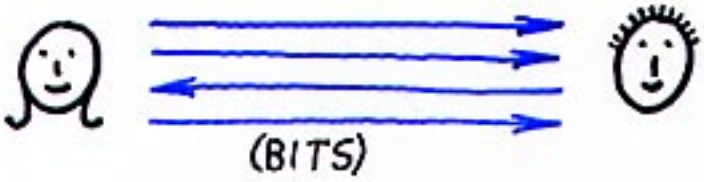
GOAL IS FOR ALICE TO CONVEY **N** BITS TO BOB



QUBIT COMMUNICATION WITH PRIOR ENTANGLEMENT:
COST IS $\frac{1}{2}$**N** [BENNETT, WIESNER '92]

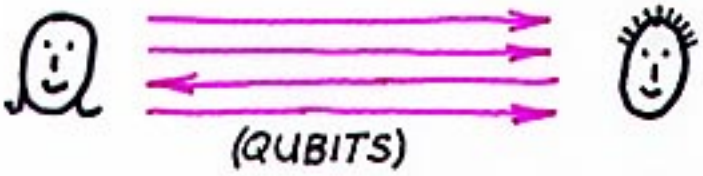
BIT COMMUNICATION

COMMUNICATION SCENARIO COSTS:



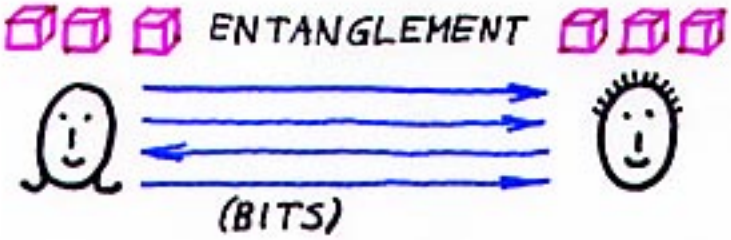
n

QUBIT COMMUNICATION



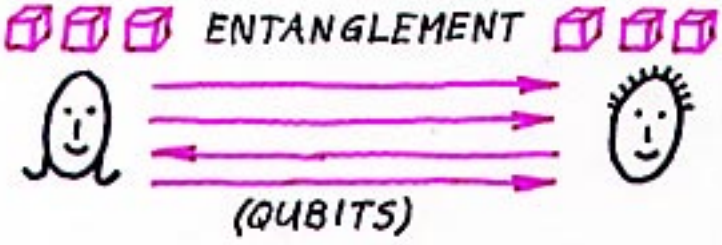
n [HOLEVO '73]

BIT COMMUNICATION WITH PRIOR ENTANGLEMENT



n [CDNT '98]

QUBIT COMMUNICATION WITH PRIOR ENTANGLEMENT



$\frac{1}{2}n$

[BENNETT&WIESNER '92]

A NON-LOCALITY SCENARIO

INPUT: X (1 BIT) Y (1 BIT)

OUTPUT: A (1 BIT) B (1 BIT)

DESIRED: $A \oplus B = X \wedge Y$

X	Y	A⊕B
0	0	0
0	1	0
1	0	0
1	1	1

EASY TO ACCOMPLISH WITH **1** BIT OF COMMUNICATION

WHAT ABOUT **0** BITS OF COMMUNICATION?

A NON-LOCALITY SCENARIO

INPUT: X (1 BIT) Y (1 BIT)

OUTPUT: A (1 BIT) B (1 BIT)

DESIRED: $A \oplus B = X \wedge Y$

X	Y	A⊕B
0	0	0
0	1	0
1	0	0
1	1	1

WITH **0** BITS OF COMMUNICATION AND:

- CLASSICAL SHARED RANDOMNESS, $PR[A \oplus B = X \wedge Y] \leq 0.75$
- QUANTUM ENTANGLEMENT, $PR[A \oplus B = X \wedge Y] \approx 0.85$

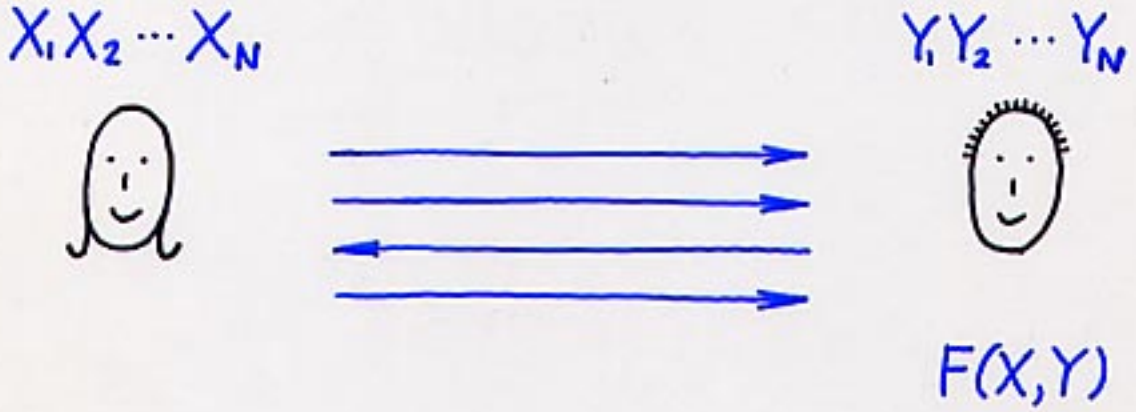
$\uparrow$

$\cos^2(\pi/8)$

2 Communication Complexity

CLASSICAL COMMUNICATION COMPLEXITY

[YAO '79]



EXAMPLE $F(X,Y) = EQ(X,Y) = \begin{cases} 1 & \text{IF } X = Y \\ 0 & \text{IF } X \neq Y \end{cases}$

- ANY DETERMINISTIC/EXACT PROTOCOL REQUIRES **N** BITS COMMUNICATION

- PROBABILISTIC/ERROR PROBABILITY ε PROTOCOLS REQUIRE ONLY $O(\log(N/\varepsilon))$ BITS COMMUNICATION

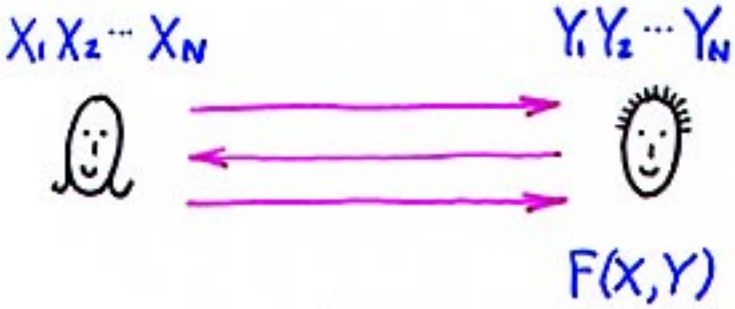
$$A(T) = X_1 + X_2 T + X_3 T^2 + \cdots + X_N T^{N-1} \pmod P$$
$$B(T) = Y_1 + Y_2 T + Y_3 T^2 + \cdots + Y_N T^{N-1} \pmod P$$

WHERE P PRIME AROUND N/ε

TEST WHETHER $A(T) \equiv B(T) \pmod P$

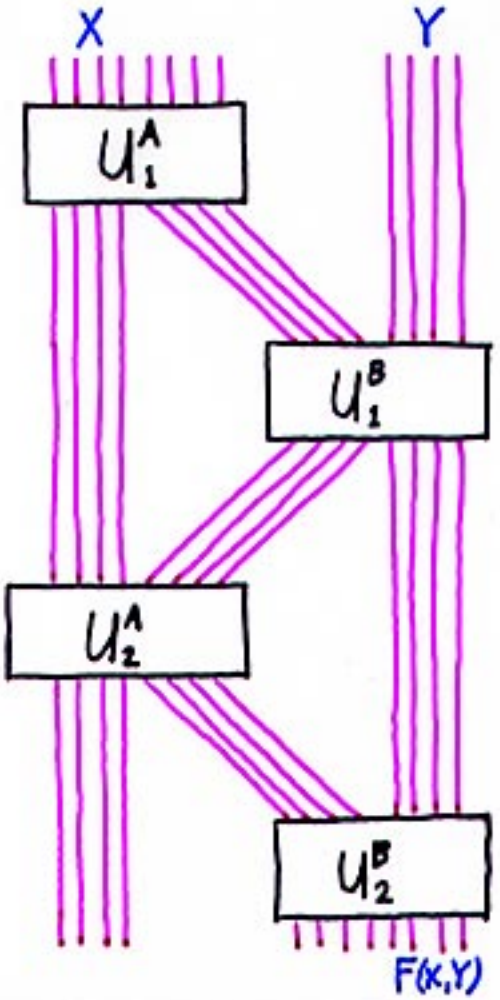
QUANTUM COMMUNICATION COMPLEXITY

QUBIT COMMUNICATION:
[YAO '93]



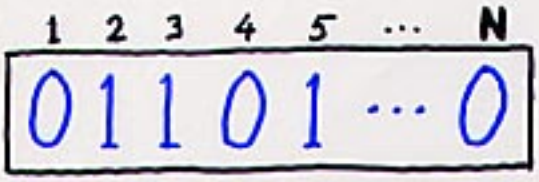
PRIOR ENTANGLEMENT:
[C, BUHRMAN '97]

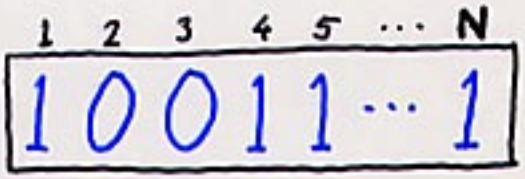
FORMAL MODEL:



INTERSECTION

"APPOINTMENT SCHEDULING"





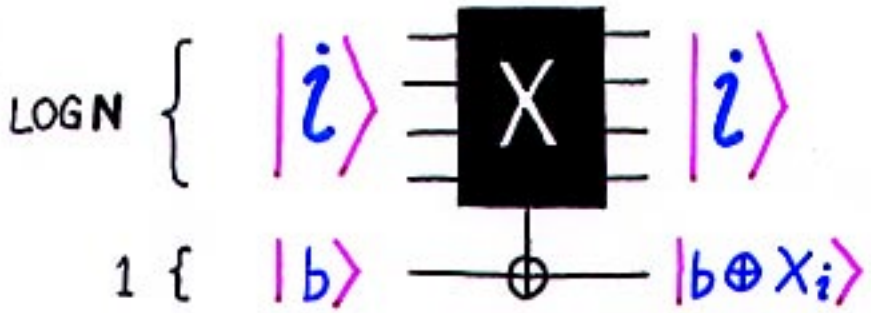
i SUCH THAT $X_i = Y_i = 1$

- CLASSICALLY, ORDER **N** BITS OF COMMUNICATION ARE NECESSARY TO SUCCEED WITH PROBABILITY $\geq \frac{2}{3}$ [KS '87]
- QUANTUM MECHANICALLY, $O(\sqrt{N})$ QUBITS OF COMMUNICATION SUFFICE TO SUCCEED WITH PROBABILITY $\geq 1-\varepsilon$ (FOR ANY $\varepsilon > 0$) [BCW '98][HdW '02][AA '03]

SEARCH PROBLEM

GIVEN: X $\boxed{\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & \cdots & N \\ 0 & 0 & 0 & 0 & 1 & 0 & \cdots & 1 \end{array}}$

ACCESSIBLE VIA QUERIES



GOAL: FIND $i \in \{1,2,\cdots,N\}$ SUCH THAT $X_i = 1$

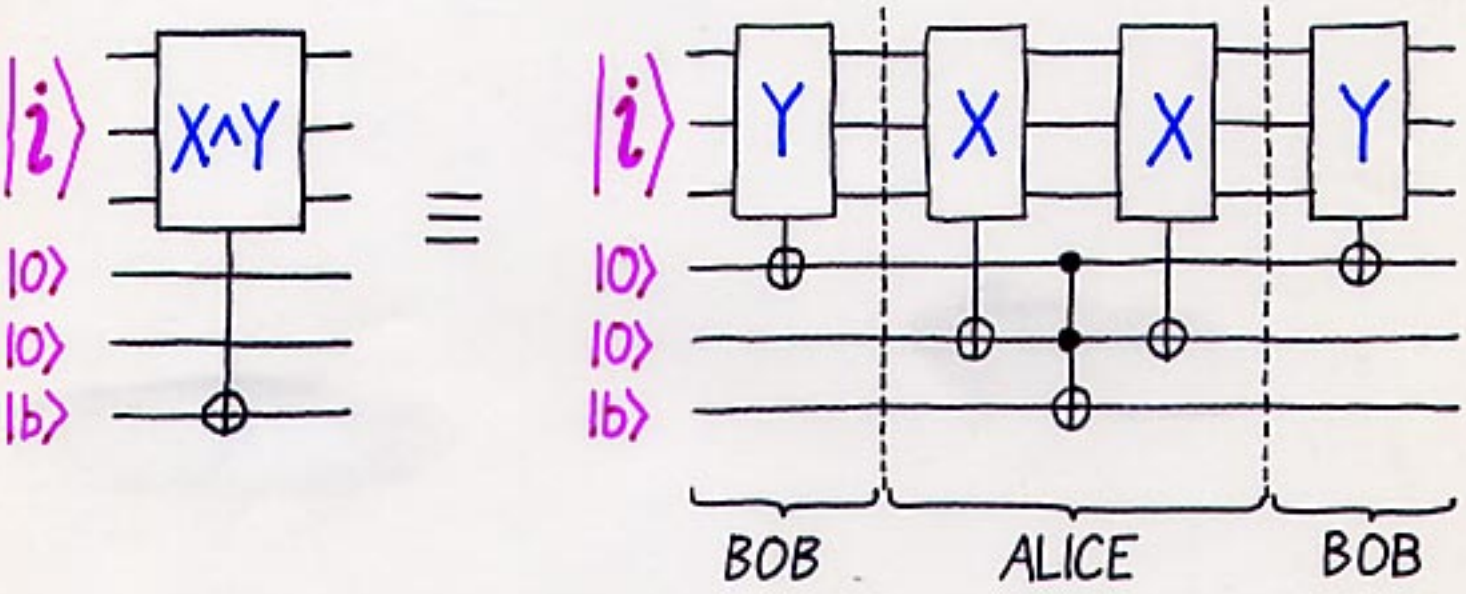
CLASSICALLY, ORDER **N** QUERIES ARE NECESSARY TO SUCCEED WITH PROBABILITY $\geq \frac{2}{3}$

FOR ALL $\varepsilon > 0$, $O(\sqrt{N})$ QUERIES SUFFICE TO SUCCEED WITH PROBABILITY $\geq 1-\varepsilon$ [GROVER '96]

"SCHEDULES": ALICE X | 1 2 3 4 5 ⋯ N | 0 1 1 0 1 ⋯ 0 |

BOB Y | 1 0 0 1 1 ⋯ 1 |

$X \wedge Y$ | 0 0 0 0 1 ⋯ 0 |



COMMUNICATION COST FOR SIMULATING ONE $X \wedge Y$-QUERY IS: $2(\log N + 3)$ QUBITS

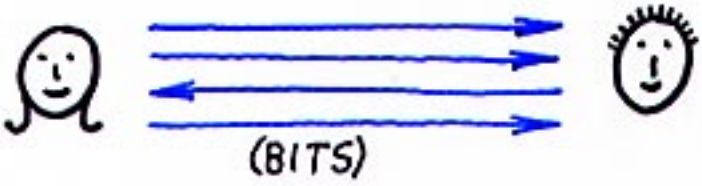
NUMBER OF $X \wedge Y$-QUERIES: $O(\sqrt{N})$ [GROVER]

TOTAL COMMUNICATION: $O(\sqrt{N} \log N)$ QUBITS

CAN BE IMPROVED TO $O(\sqrt{N})$, WHICH IS OPTIMAL [RAZBOROV '02]

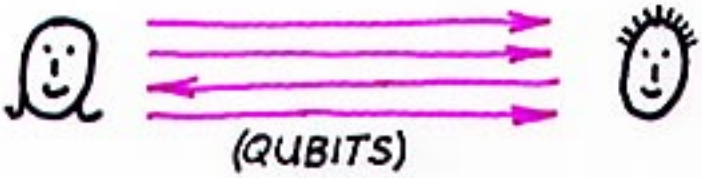
BIT COMMUNICATION

INTERSECTION PROBLEM
COMMUNICATION COSTS



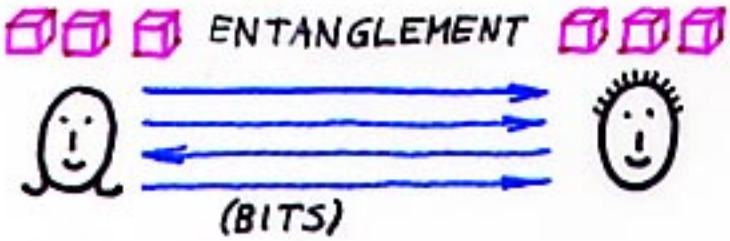
$\Omega(N)$

QUBIT COMMUNICATION



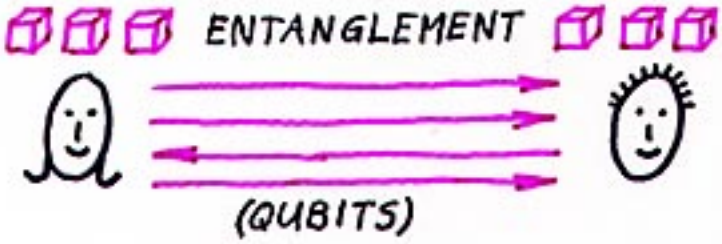
$O(\sqrt{N})$

BIT COMMUNICATION WITH PRIOR ENTANGLEMENT



$O(\sqrt{N})$

QUBIT COMMUNICATION WITH PRIOR ENTANGLEMENT



$O(\sqrt{N})$

OTHER QUANTUM VS CLASSICAL COMMUNICATION COMPLEXITY RESULTS

- $O(\log \mathbf{N})$ QUANTUM VS ORDER $\mathbf{N}$ CLASSICAL FOR <u>EXACT</u> PROTOCOLS [B,C,W '98]
- $O(\log \mathbf{N})$ QUANTUM VS ORDER $\approx \mathbf{N}^{\frac{1}{4}}$ CLASSICAL FOR <u>BOUNDED-ERROR</u> ($\leq \varepsilon$) PROTOCOLS [RAZ '99]

INNER-PRODUCT

$IP(X,Y) = X_1 Y_1 + X_2 Y_2 + \cdots + X_N Y_N$ (MODULO 2)

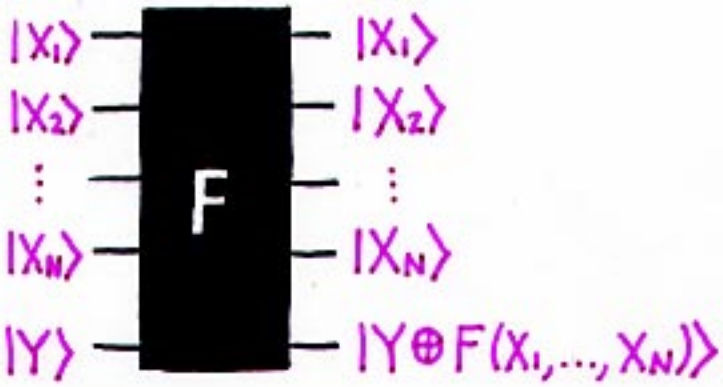
ORDER **N** COMMUNICATION NECESSARY FOR BOTH QUANTUM AND CLASSICAL PROTOCOLS [KY '95][CDNT '97]

MULTI-LINEAR INTERPOLATION PROBLEM

$F: \{0,1\}^N \rightarrow \{0,1\}$

$F(X_1, \ldots, X_N) = A_1 X_1 + A_2 X_2 + \cdots + A_N X_N \mod 2$

GIVEN:



GOAL: DETERMINE $A_1, A_2, \ldots, A_N$

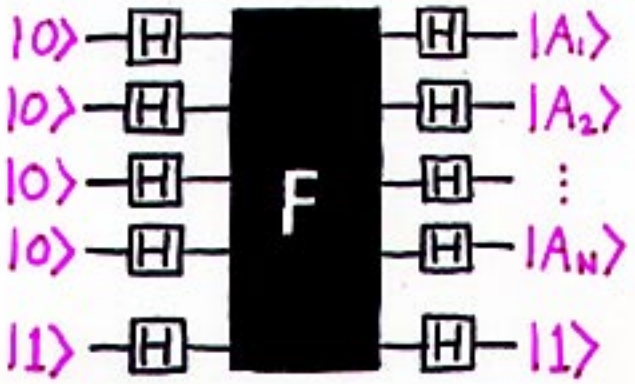
CLASSICALLY, **N** *QUERIES NECESSARY*

MULTI-LINEAR INTERPOLATION PROBLEM

$F: \{0,1\}^N \rightarrow \{0,1\}$

$F(X_1, \ldots, X_N) = A_1 X_1 + A_2 X_2 + \cdots + A_N X_N \mod 2$

GIVEN:



$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

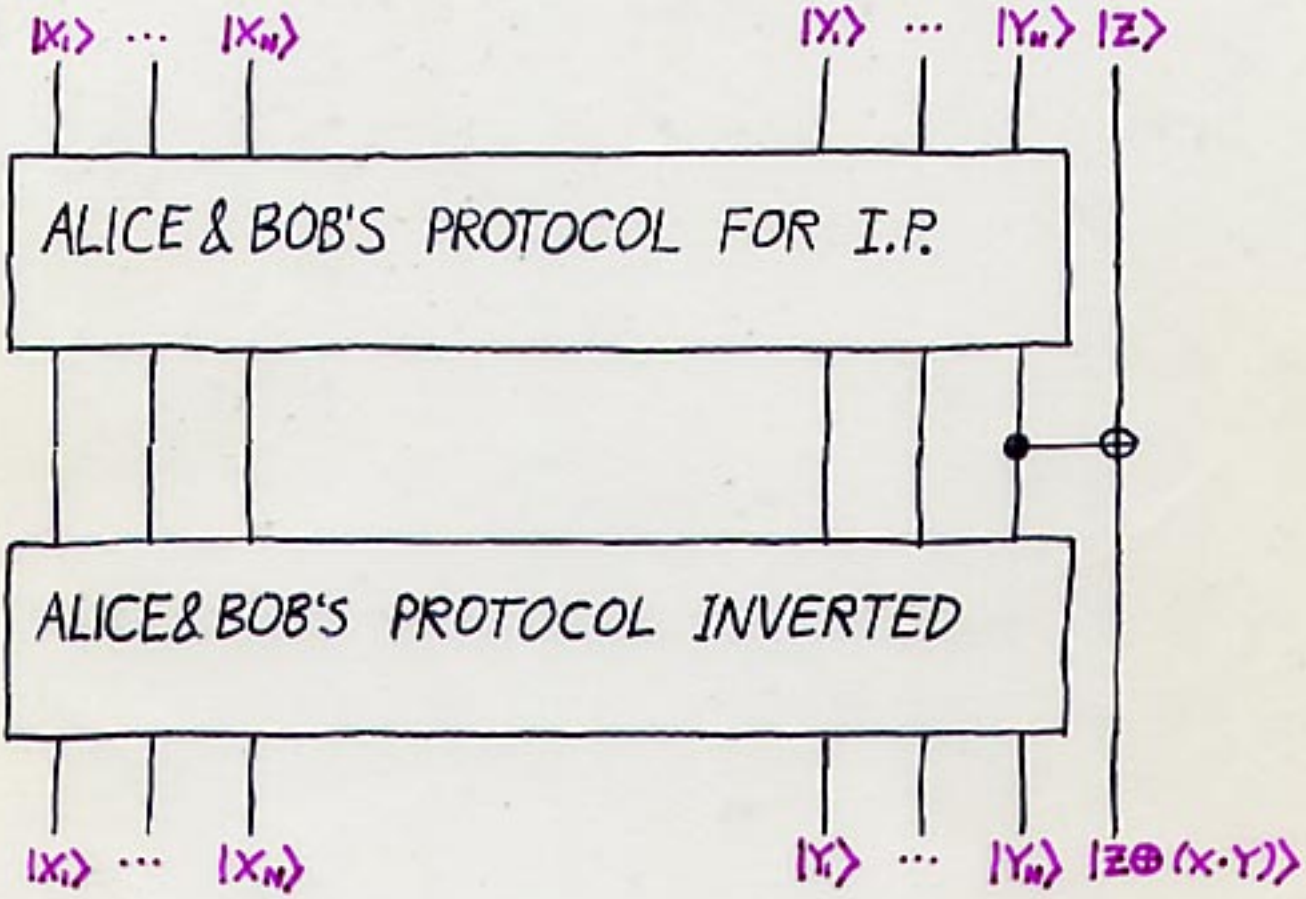
GOAL: DETERMINE $A_1, A_2, \ldots, A_N$

CLASSICALLY, **N** QUERIES NECESSARY

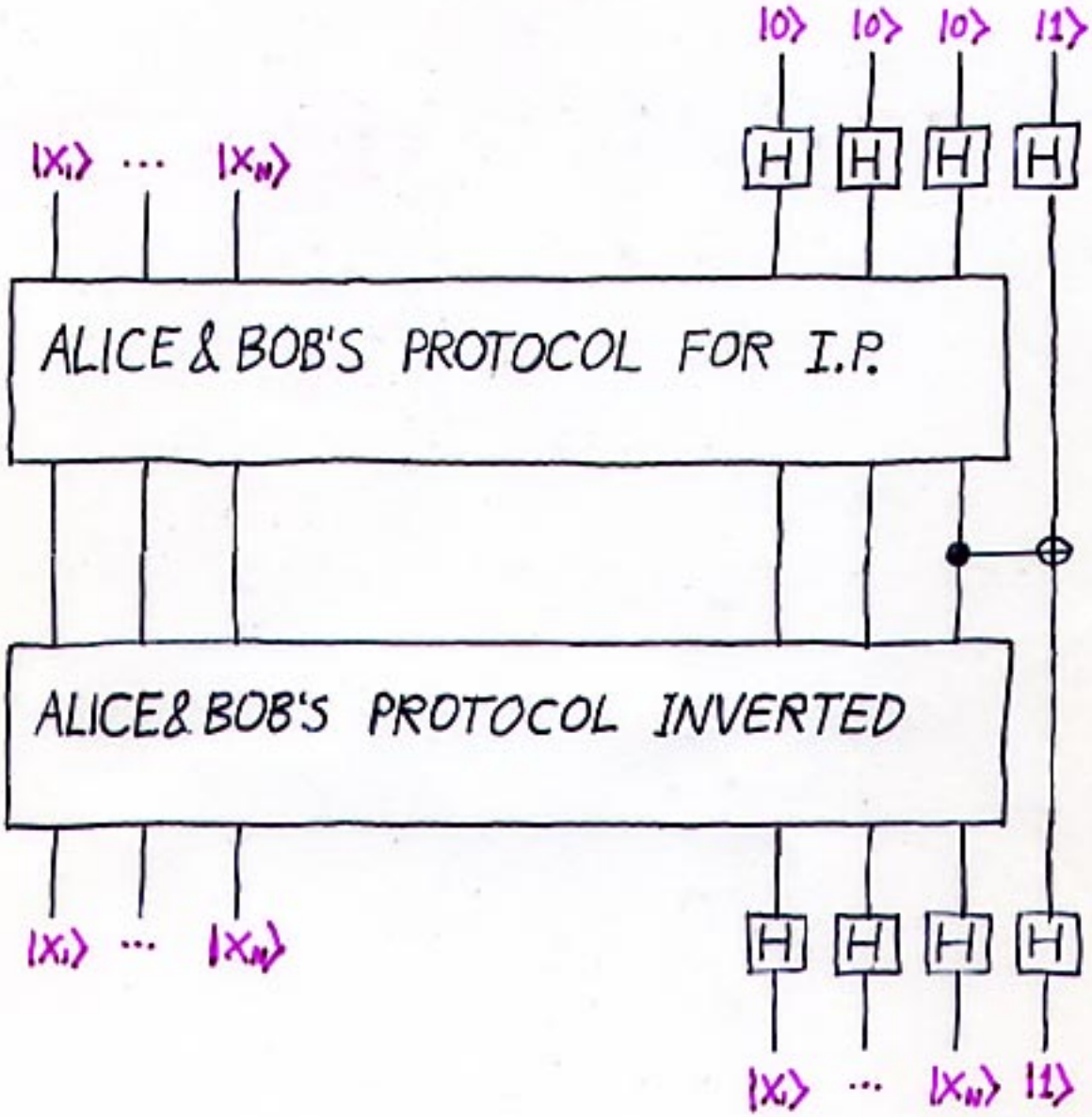
"QUANTUMLY," **1** QUERY SUFFICIENT

[BERNSTEIN, VAZIRANI '93][TERHAL, SMOLIN '97]

PROOF THAT N QUBITS COMMUNICATION ARE NECESSARY FOR INNER PRODUCT



PROOF THAT N QUBITS COMMUNICATION ARE NECESSARY FOR INNER PRODUCT

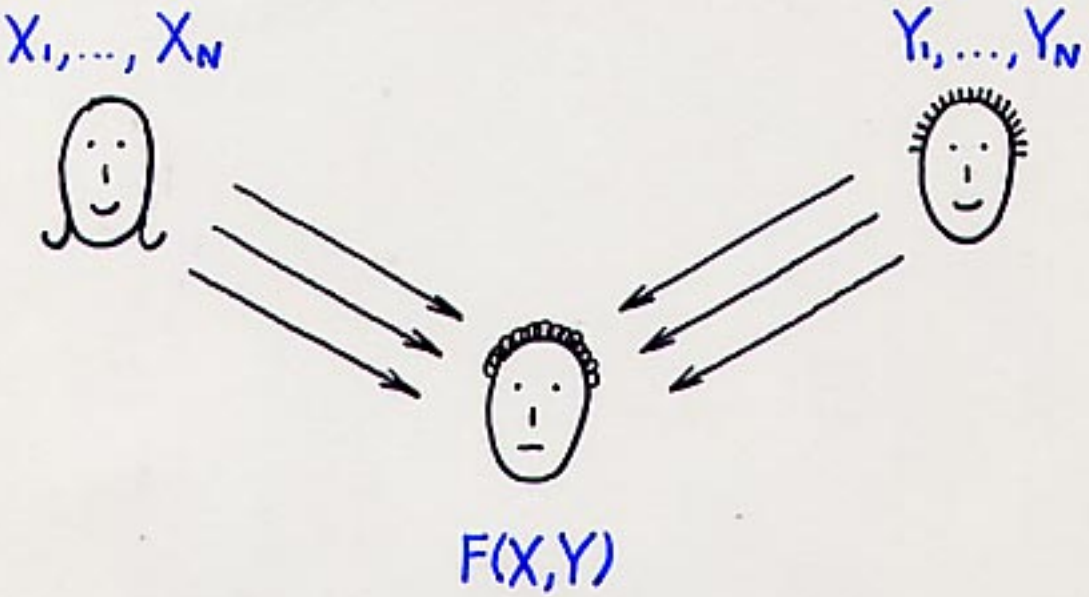


SINCE **N** BITS ARE CONVEYED FROM ALICE TO BOB, **Ω(N)** QUBITS COMMUNICATION MUST OCCUR (BY HOLEVO'S THEOREM)

3 Variations

EQUALITY REVISITED

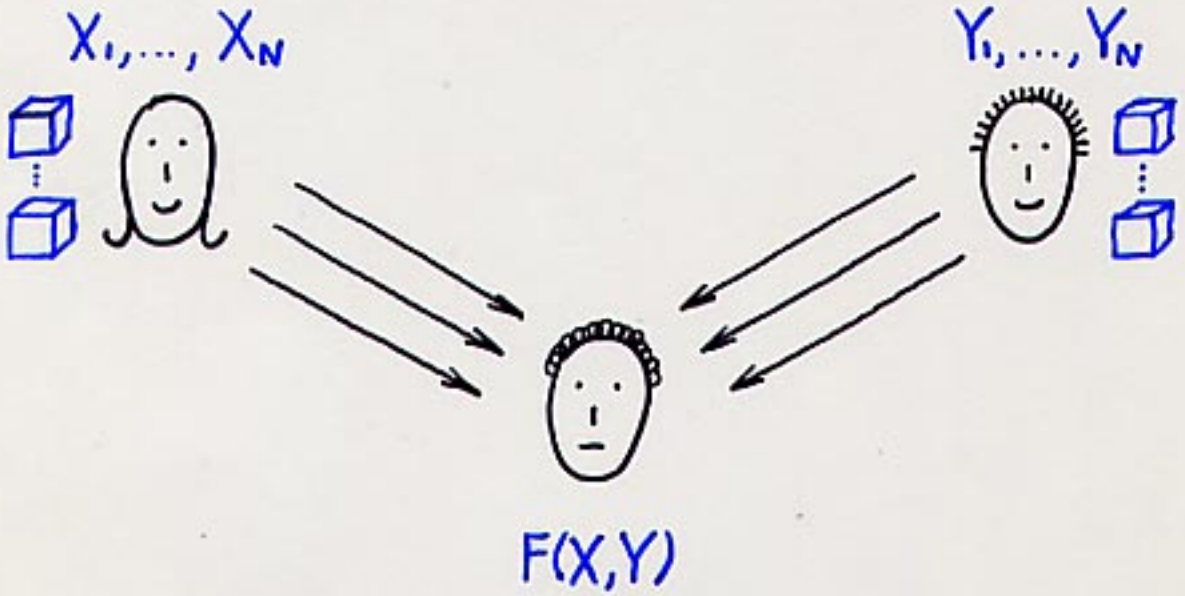
IN THE SIMULTANEOUS MESSAGE MODEL



EXACT PROTOCOLS REQUIRE **2N** BITS/QUBITS COMMUNICATION

EQUALITY REVISITED

IN THE SIMULTANEOUS MESSAGE MODEL



BOUNDED-ERROR PROTOCOLS WITH A SHARED KEY

$PR[00] = PR[11] = \frac{1}{2}$

REQUIRE ONLY A <u>CONSTANT</u> NUMBER OF <u>BITS</u> OF COMMUNICATION

ERROR-CORRECTING CODE:

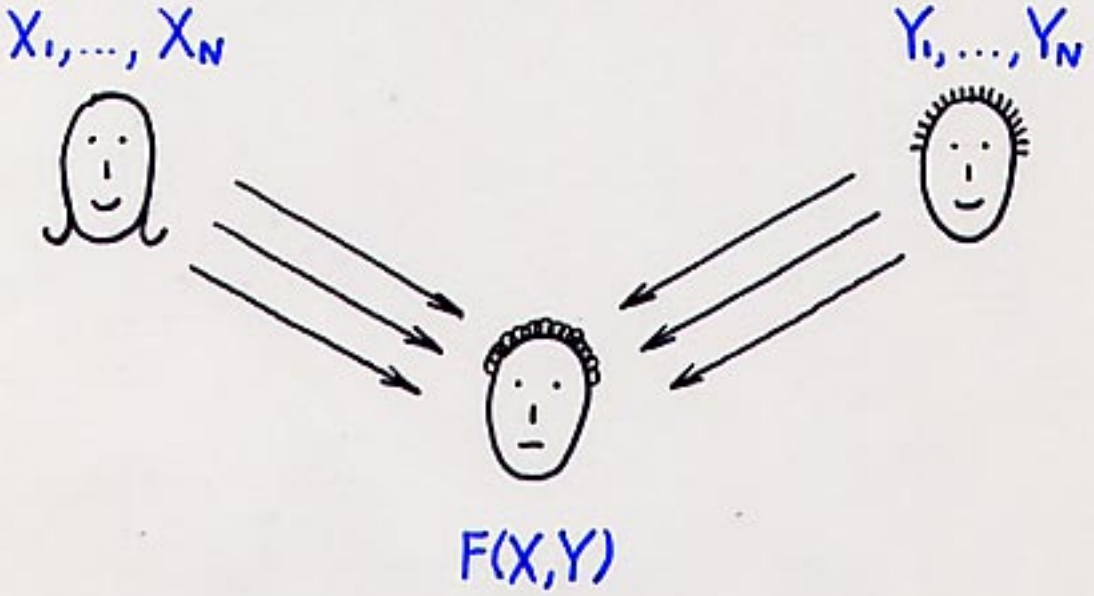
$C(X) =$ 1 0 1 1 1 1 0 1 0 1 1 0 0 1 1 0 LENGTH $O(N)$

$C(Y) =$ 0 1 1 0 1 0 0 1 0 0 1 1 0 0 1 0

K $O(\log N)$ BITS

EQUALITY REVISITED

IN THE SIMULTANEOUS MESSAGE MODEL



BOUNDED-ERROR PROTOCOLS WITHOUT A SHARED KEY

- CLASSICAL: ORDER $\sqrt{N}$ BITS [A '96][NS '96]
- QUANTUM: ORDER **LOGN** BITS [BCWdW '01]

QUANTUM FINGERPRINTS

- HOW MANY ORTHOGONAL STATES IN $K = \log N + O(1)$ QUBITS?

  ANSWER: $2^K = O(N)$

- HOW MANY ALMOST* ORTHOGONAL STATES IN $K = \log N + O(1)$ QUBITS? (* $|\langle \phi_x | \phi_y \rangle| \leq \varepsilon$)

  ANSWER:

QUANTUM FINGERPRINTS

- HOW MANY ORTHOGONAL STATES IN $K = \log N + O(1)$ QUBITS?
  ANSWER: $2^K = O(N)$

- HOW MANY ALMOST* ORTHOGONAL STATES IN $K = \log N + O(1)$ QUBITS? (* $|\langle \phi_x | \phi_y \rangle| \leq \varepsilon$)
  ANSWER: $2^{2^{K-O(1)}} = 2^N$

- DOES THIS ENABLE N BITS TO BE "COMPRESSED" INTO $\log N + O(1)$ QUBITS?
  ANSWER:

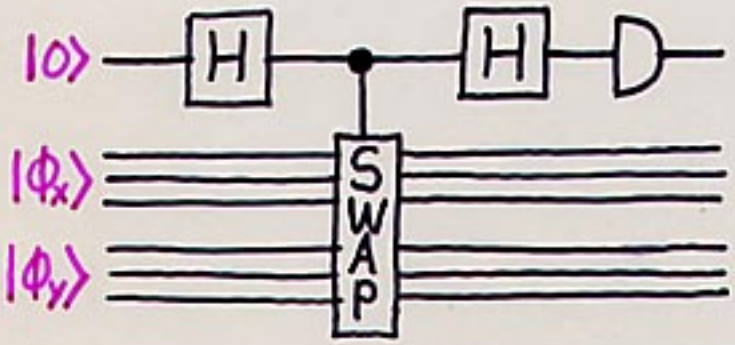
QUANTUM FINGERPRINTS

- HOW MANY ORTHOGONAL STATES IN $K = \log N + O(1)$ QUBITS?
  ANSWER: $2^K = O(N)$

- HOW MANY ALMOST* ORTHOGONAL STATES IN $K = \log N + O(1)$ QUBITS? ($* \; |\langle \phi_x | \phi_y \rangle| \leq \varepsilon$)
  ANSWER: $2^{2^{K-O(1)}} = 2^N$

- DOES THIS ENABLE N BITS TO BE "COMPRESSED" INTO $\log N + O(1)$ QUBITS?
  ANSWER: NO! – HOLEVO'S THEOREM

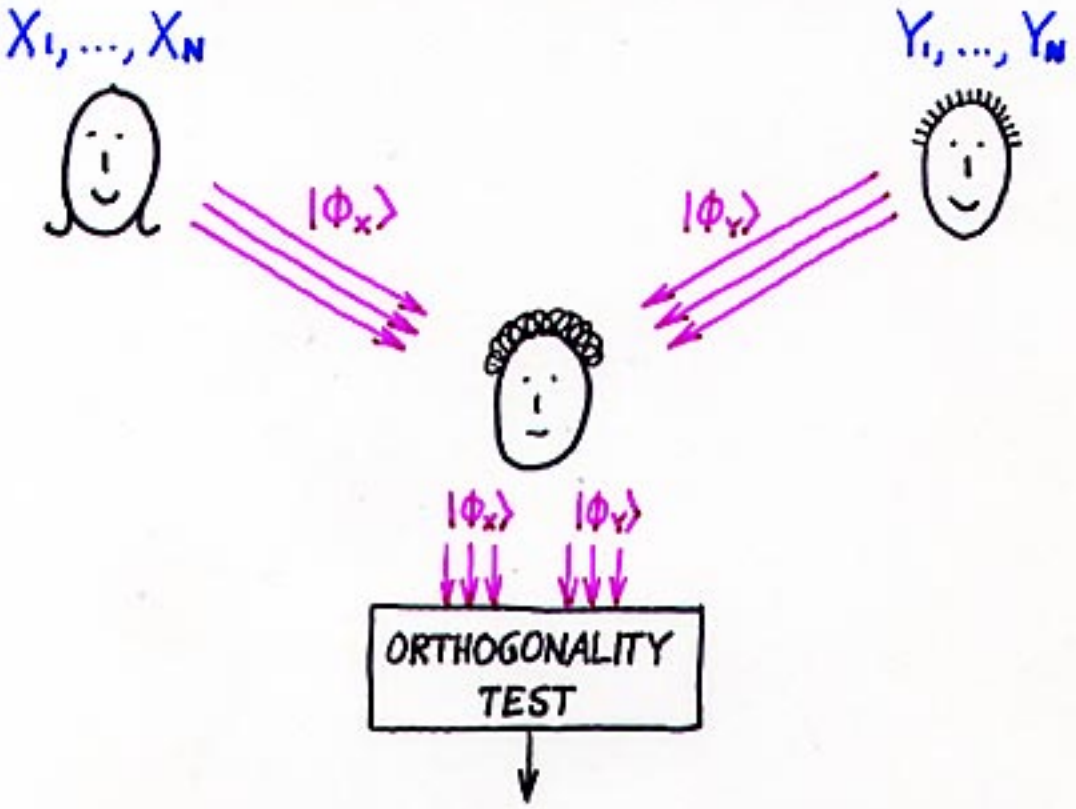
- HOWEVER, IT DOES ENABLE ONE TO CHECK IF $X = Y$ OR $X \neq Y$ BY ONLY EXAMINING $|\phi_x\rangle$, $|\phi_y\rangle$



$$\text{PR}[\text{OUTPUT}=0] = \begin{cases} 1 & \text{IF } X = Y \\ \frac{1}{2}(1+\varepsilon^2) & \text{IF } X \neq Y \end{cases}$$

QUANTUM PROTOCOL FOR EQUALITY

IN THE SIMULTANEOUS MESSAGE MODEL



$O(\log N)$ QUBITS vs. $\Theta(\sqrt{N})$ BITS CLASSICALLY

RESTRICTED EQUALITY REVISITED

WITH DISTRIBUTED OUTPUTS

EXAMPLE [BRASSARD, C, TAPP '99]

INPUT: X (**N** BITS) Y (**N** BITS)

OUTPUT: A ($\log$ **N** BITS) B ($\log$ **N** BITS)

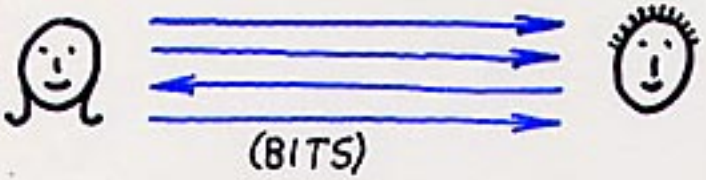
PRECONDITION: $X = Y$ OR $\Delta(X,Y) = \frac{1}{2}\mathbf{N}$

REQUIRED POSTCONDITION (EXACT): $\begin{cases} A = B & \text{IF } X = Y \\ A \neq B & \text{IF } X \neq Y \end{cases}$

- CLASSICALLY, $\Omega(\mathbf{N})$ BITS COMMUNICATION NECESSARY
- WITH $\log$**N** PAIRS OF ENTANGLED QUBITS, NO COMMUNICATION NEEDED AT ALL!

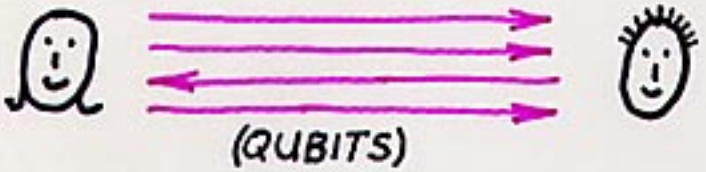
BIT COMMUNICATION

[BCT '99]



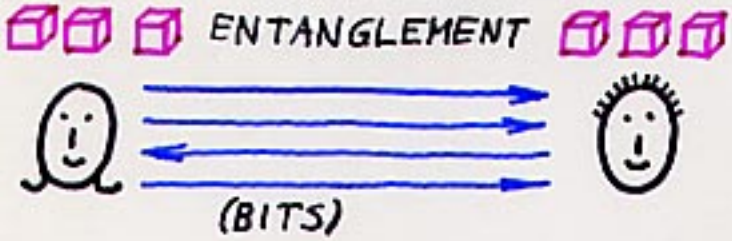
$\Omega(N)$

QUBIT COMMUNICATION



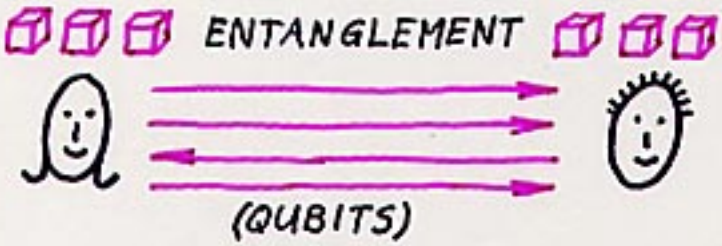
$O(\text{LOG}(N))$

BIT COMMUNICATION WITH PRIOR ENTANGLEMENT



ZERO

QUBIT COMMUNICATION WITH PRIOR ENTANGLEMENT



ZERO

CONCLUSIONS

- QUANTUM INFORMATION AFFECTS COMMUNICATION COMPLEXITY IN AN INTERESTING WAY

- LOTS OF INTERPLAY BETWEEN COMMUNICATION COMPLEXITY AND:
  - INFORMATION THEORY
  - COMPLEXITY THEORY
  - BELL NONLOCALITY