

An Introduction to
Quantum Information and
Applications



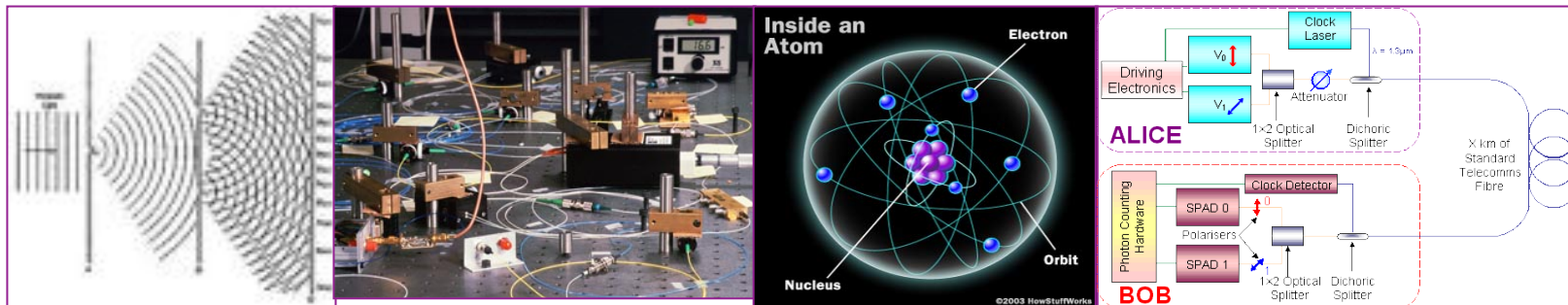
Jordanis Kerenidis

CNRS

LIAFA-Univ Paris-Diderot

Quantum information and computation

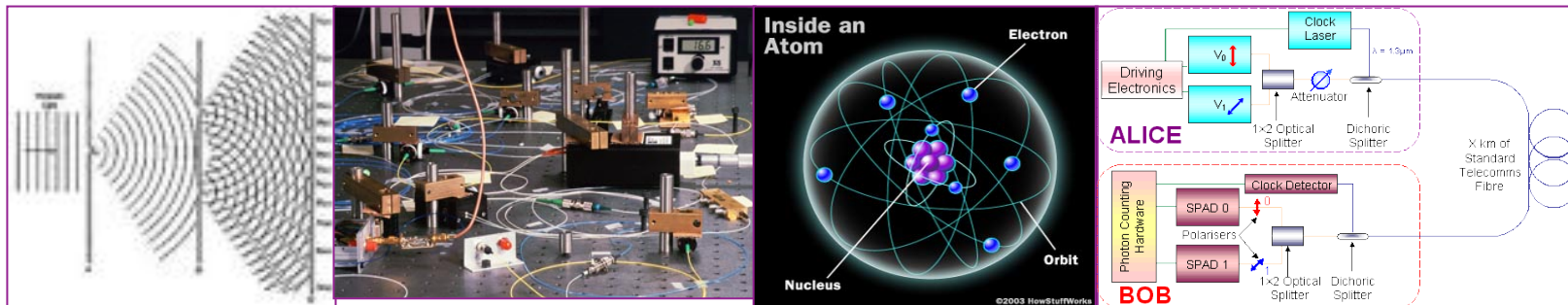
- Quantum information and computation
 - How is information encoded in nature?
 - What is nature's computational power?
- Moore's law: quantum phenomena will appear by 2020
- Rich Mathematical Theory
 - Advances in Classical Computer Science
 - Advances in Theoretical & Experimental Physics
 - Advances in Information Theory



Quantum information and computation

The power of Quantum Computing

- Quantum algorithm for Factoring and Discrete Logarithm [Shor 93]
- Unconditionally Secure Key Distribution [Bennett-Brassard 84]
- Quantum computers unlikely to solve NP-complete problems [Bernstein Bennett Brassard Vazirani 94]



Outline

1) Introduction to the model

- Superdense Coding
- Teleportation

2) Basic algorithms

- Deutsch-Jozsa
- Ideas for Factoring

3) Cryptography

- Key Distribution

4) Communication Complexity

- Quantum fingerprints
- Exponential Separations

Quantum States

- Quantum bit is a unit vector in a 2-dim. Hilbert space \mathcal{H}

$$a_0|0\rangle + a_1|1\rangle, \quad a_0, a_1 \in \mathcal{C}, \quad |a_0|^2 + |a_1|^2 = 1$$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

- A quantum state on $\log n$ qubits is a unit vector in $\mathcal{H}^{\otimes \log n}$

$$|\phi\rangle = \sum_{i=0}^{n-1} a_i |i\rangle, \quad \sum_{i=0}^{n-1} |a_i|^2 = 1 \quad |\varphi\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \quad \langle\varphi| = (a_1 \ a_2 \ \cdots \ a_n)$$

- Inner product: $\langle\varphi|\psi\rangle$

Measurements on Quantum States

- A measurement of $|\phi\rangle$ in an orthonormal basis $\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$ is a projection onto the basis vectors and

$$\text{Pr}[\text{outcome is } b_i] = |\langle \phi | b_i \rangle|^2$$

- Examples

$$|\phi\rangle = a_0|0\rangle + a_1|1\rangle, \quad \{|0\rangle, |1\rangle\}$$

$$\text{Prob}[\text{outcome } |0\rangle] = |\langle 0 | \phi \rangle|^2 = |a_0 \langle 0 | 0 \rangle + a_1 \langle 0 | 1 \rangle|^2 = |a_0|^2$$

$$\text{Prob}[\text{outcome } |1\rangle] = |\langle 1 | \phi \rangle|^2 = |a_0 \langle 1 | 0 \rangle + a_1 \langle 1 | 1 \rangle|^2 = |a_1|^2$$

Measurements on Quantum States

- A measurement of $|\phi\rangle$ in an orthonormal basis $\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$ is a projection onto the basis vectors and

$$\text{Pr}[\text{outcome is } b_i] = |\langle \phi | b_i \rangle|^2$$

- Examples

$$|\phi\rangle = a_0|0\rangle + a_1|1\rangle, \quad \left\{ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right\}$$

$$\text{Prob}[\text{outcome } \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)] = \left| \frac{1}{\sqrt{2}} a_0 \langle 0|0\rangle + \frac{1}{\sqrt{2}} a_1 \langle 1|1\rangle \right|^2 = \frac{1}{2} + a_0 a_1$$

$$\text{Prob}[\text{outcome } \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)] = \left| \frac{1}{\sqrt{2}} a_0 \langle 0|0\rangle - \frac{1}{\sqrt{2}} a_1 \langle 1|1\rangle \right|^2 = \frac{1}{2} - a_0 a_1$$

Measurements on Quantum States

- A measurement of $|\phi\rangle$ in an orthonormal basis $\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$ is a projection onto the basis vectors and

$$\Pr[\text{outcome is } b_i] = |\langle \phi | b_i \rangle|^2$$

- Examples

$$|\phi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle, \quad \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

$$\Pr ob[\text{outcome } |00\rangle] = |a_{00}|^2$$

- Note that $|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

Measurements on Quantum States

- A measurement of $|\phi\rangle$ in an orthonormal basis $\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$ is a projection onto the basis vectors and

$$\Pr[\text{outcome is } b_i] = |\langle \phi | b_i \rangle|^2$$

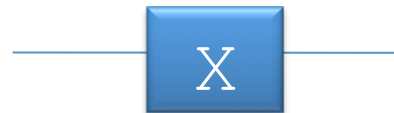
- **IMPORTANT REMARK**
 - What is the final state after the measurement?
 - The state changes to the basis state
 - Hence, no more information in it about the a_i 's.
 - If I repeat the measurement I always get the same basis vector.

Unitary Evolution

- Unitary matrix: inner product/length preserving, linear

$$U|\varphi\rangle = U\left(\sum_{i=0}^{n-1} a_i|i\rangle\right) = \sum_{i=0}^{n-1} a_i U|i\rangle$$

- NOT gate



$$|0\rangle \xrightarrow{X} |1\rangle \quad , \quad |1\rangle \xrightarrow{X} |0\rangle$$

- Phase Flip gate




$$|0\rangle \xrightarrow{Z} |0\rangle \quad , \quad |1\rangle \xrightarrow{Z} -|1\rangle$$

Unitary Evolution cont.


- Hadamard Gate 

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad , \quad |1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- Control NOT gate 

$$|00\rangle \xrightarrow{CNOT} |00\rangle, |01\rangle \xrightarrow{CNOT} |01\rangle,$$

$$|10\rangle \xrightarrow{CNOT} |11\rangle, |11\rangle \xrightarrow{CNOT} |10\rangle$$

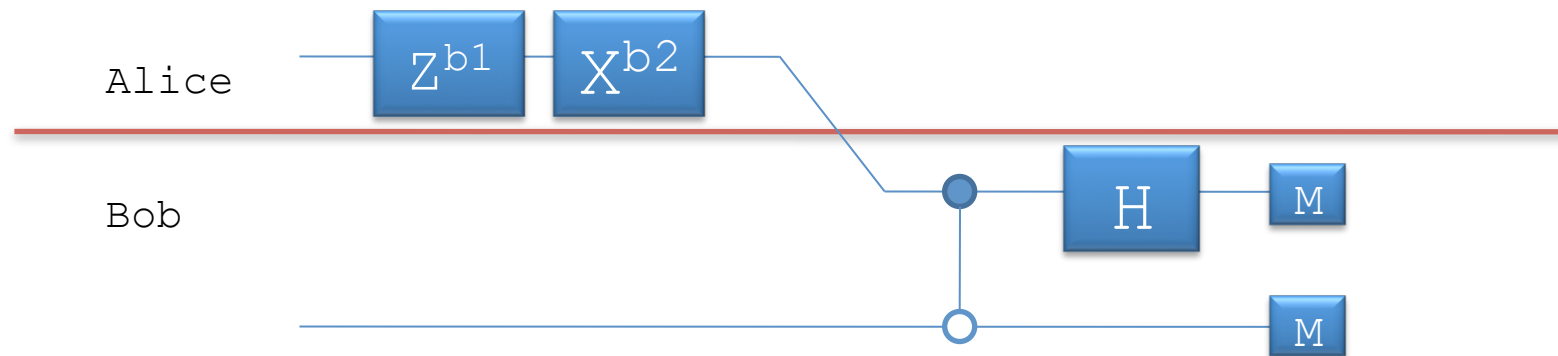
- Example 

$$|0\rangle \otimes |0\rangle \equiv |0\rangle|0\rangle \equiv |00\rangle$$

$$|0\rangle \otimes |0\rangle \xrightarrow{H \text{ on } 1st} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$$

Superdense Coding

- Transmitting 2 bits with 1 qubit
 - Alice and Bob share the above state $\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$
 - Alice wants to transmit the bits b_1b_2 to Bob

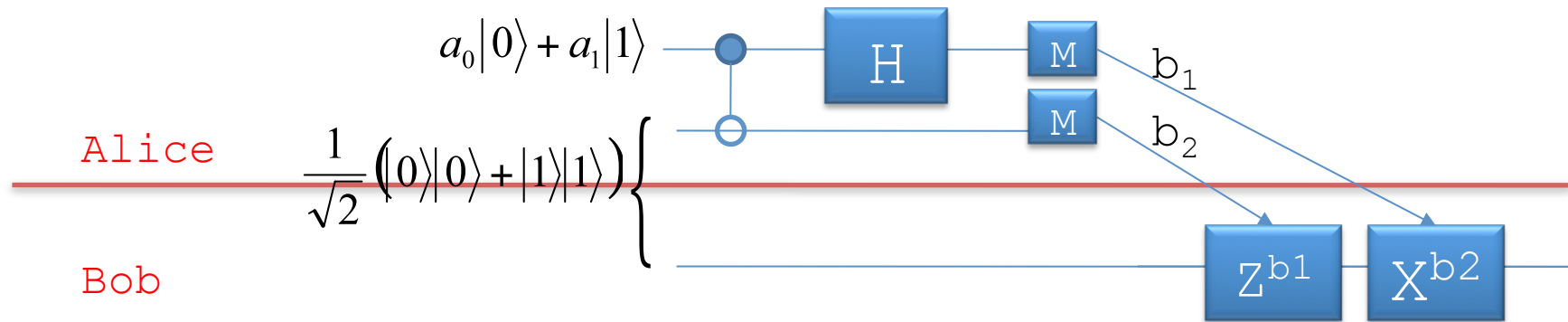


- Let $b_1b_2=10$

$$\begin{aligned}
 & \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \xrightarrow{Z \text{ if } b_1=1} \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle) \xrightarrow{X \text{ if } b_2=1} \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle) \\
 & \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|0\rangle) \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|0\rangle \xrightarrow{H \text{ on 1st}} |1\rangle|0\rangle
 \end{aligned}$$

Teleportation

- Teleporting a qubit with 2 bits
 - Alice and Bob share the state $\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$
 - Alice wants to transmit an unknown qubit to Bob



$$(a_0|0\rangle + a_1|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(a_0|000\rangle + a_1|110\rangle + a_0|011\rangle + a_1|101\rangle)$$

$$\xrightarrow{H} \frac{1}{2}|00\rangle(a_0|0\rangle + a_1|1\rangle) + \frac{1}{2}|01\rangle(a_0|1\rangle + a_1|0\rangle) + \frac{1}{2}|10\rangle(a_0|0\rangle - a_1|1\rangle) + \frac{1}{2}|11\rangle(a_0|1\rangle - a_1|0\rangle)$$

$$\xrightarrow{Z^{b_1} X^{b_2}} (a_0|0\rangle + a_1|1\rangle)$$

Outline

- 1) Introduction to the model
 - Superdense Coding
 - Teleportation

- 2) Basic algorithms
 - Deutsch-Jozsa
 - Ideas for Factoring

- 3) Cryptography
 - Key Distribution

- 4) Communication Complexity
 - Quantum fingerprints
 - Exponential Separations

Quantum Queries

Let $f: X \rightarrow Y$

Goal: Does f have a certain property?

Classical Query: "What is the value of $f(x)$?"

$$x \xrightarrow{O_f} f(x)$$

Example: Is f linear or far from linear?

3 Queries u.a.r.: $f(x), f(y), f(x+y)$. Check $f(x) + f(y) = f(x+y)$

Quantum Query

$$|x\rangle|b\rangle \xrightarrow{O_f} |x\rangle|b \oplus f(x)\rangle$$

But, quantum operations are linear!

$$|0\dots 0\rangle|0\rangle \xrightarrow{H} \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |0\rangle \xrightarrow{O_f} \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$$

Deutsch-Jozsa Algorithm

Let $f: \{0,1\}^n \rightarrow \{0,1\}$

Goal: Is f identically zero or balanced?

Classical Query: $x \xrightarrow{O_f} f(x)$

deterministic: $2^{n-1}+1$

randomized: k queries, error probability 2^{-k}

Quantum $|x\rangle|b\rangle \xrightarrow{O_f} |x\rangle|b \oplus f(x)\rangle$

$$|0\dots 0\rangle|0\rangle \xrightarrow{H} \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle|0\rangle \xrightarrow{O_f} \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle|f(x)\rangle$$

$$\xrightarrow{Z \text{ on } 2nd} \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle|f(x)\rangle \xrightarrow{O_f} \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle|0\rangle$$

$$\xrightarrow{H} \begin{cases} |0\dots 0\rangle & \text{if } f = 0 \\ \sum_{y \in \{0,1\}^n} a_y |y\rangle, \text{ with } a_0 = 0, & \text{if } f \text{ balanced} \end{cases}$$

More Algorithms

- Simon's problem

Let $f: \{0,1\}^n \rightarrow \{0,1\}^n$

Promise: $f(x) = f(x+a)$ and $f(x) \neq f(y)$, $y \neq x+a$ (2-periodic)

Goal: Find a

Randomized: $2^{n/2}$

Quantum: $O(n)$, by finding each time a random y , st. $y \cdot a = 0$

- Period Finding [Shor94]

Let $f: \mathbb{Z}_N \rightarrow \mathbb{C}$

Promise: f is periodic

Goal: Find period

Quantum: Easy algorithm, based on Fourier Transform

Factoring = Period Finding !

- Search an unordered list: $O(\sqrt{n})$ queries [Grover97]

2) Algorithms: Open Problems

- Find New Algorithms
 - Graph Isomorphism?
 - Lattice Problems?
 - Hidden Subgroup Problems?
 - other...
- Exponential speedup (possibly)
 - Factoring, Discrete Log, Pell's Equality, ...
- Quadratic speedup (provably)
 - Grover's Search, Quantum walk-based algorithms, ...

Outline

- 1) Introduction to the model
 - Superdense Coding
 - Teleportation

- 2) Basic algorithms
 - Deutsch-Jozsa
 - Ideas for Unordered search and Factoring

- 3) Cryptography
 - Key Distribution

- 4) Communication Complexity
 - Quantum fingerprints
 - Exponential Separations

3) Cryptography



- Current cryptography based on computational assumptions (e.g. hardness of factoring)
- Many such problems become insecure against a quantum adversary
- Can we use quantum interaction to achieve unconditionally secure cryptography?

Unconditional Key Distribution



1. Alice picks a secret key.
She encodes each bit in one
of two possible quantum ways
and sends it to Bob.

2. Bob guesses the encoding and
decodes each bit accordingly

Remarks:

- If Bob guesses correctly the encoding, then the decoding is perfect. If not, Bob gets a random bit.
- Bob guesses correctly half the times.

Unconditional Key Distribution



1. Alice picks a secret key.
She encodes each bit in one
of two possible quantum ways
and sends it to Bob.

2. Bob guesses the encoding and
decodes each bit accordingly

3. Alice and Bob reveal publicly the encodings
and keep only the bits on which they agree. (~ half)

Remarks: - If there is no Eve, then they agree on the value
of all these bits.
- If Eve has got information about the key, then with high
probability Alice and Bob will disagree on some bits.

Unconditional Key Distribution



1. Alice picks a secret key.
She encodes each bit in one of two possible quantum ways and sends it to Bob.
2. Bob guesses the encoding and decodes each bit accordingly
3. Alice and Bob reveal publicly the encodings and keep only the bits on which they agree. (~ half)
4. Alice and Bob reveal publicly the values of half of the bits (1/4 of the initial).
 - If they agree, they use the rest as the key (~ 1/4)
 - If they disagree in many bits, they throw it away

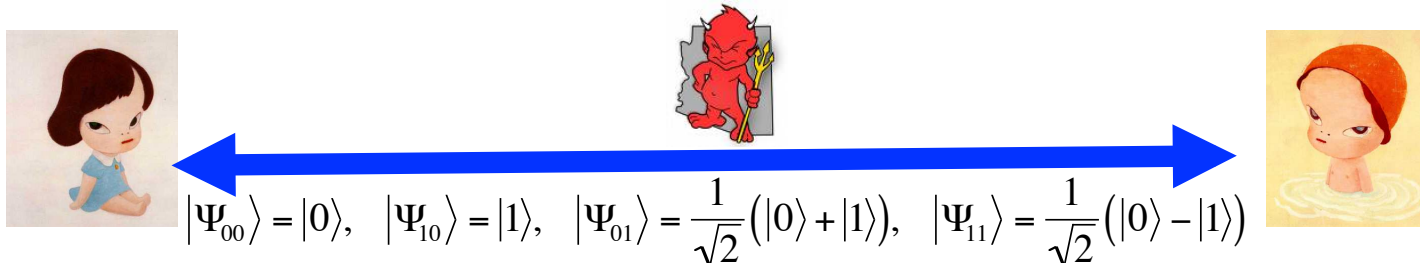
Unconditional Key Distribution



$$|\Psi_{00}\rangle = |0\rangle, \quad |\Psi_{10}\rangle = |1\rangle, \quad |\Psi_{01}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |\Psi_{11}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

1. Pick $a, b \in \{0, 1\}^n$
(a : key | b : encoding)
Send each $|\Psi_{a_i b_i}\rangle$
2. Pick $b' \in \{0, 1\}^n$
If $b_i = 0$ measure in $\{|\Psi_{00}\rangle, |\Psi_{10}\rangle\}$
If $b_i = 1$ measure in $\{|\Psi_{01}\rangle, |\Psi_{11}\rangle\}$
Denote outcome a_i
3. Alice and Bob reveal publicly the encodings b, b' .
Keep the bits for which $b_i = b'_i$ (\sim half)
4. Alice and Bob reveal publicly the values of $a_i = a'_i$
for half of the bits for which $b_i = b'_i$
 - If they agree, they use the rest as the key ($\sim 1/4$)
 - If they disagree in many bits, they throw it away

Unconditional Key Distribution



Proof of Security (idea)

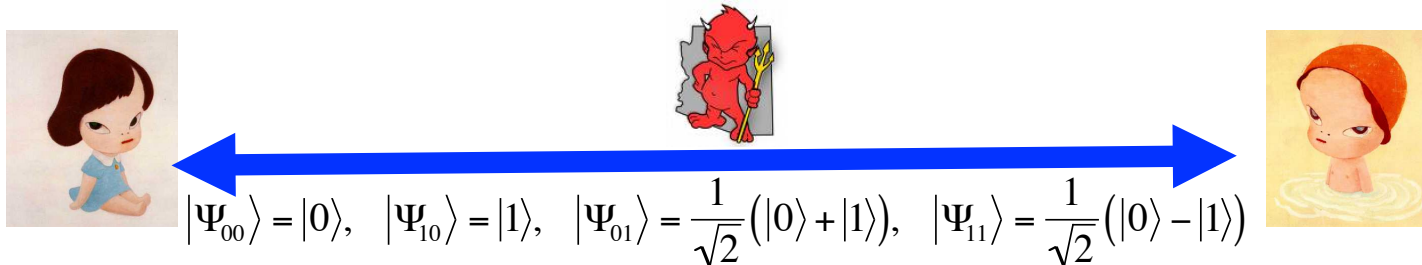
- Eve gets information, she disturbs the state (Heisenberg)

Possible strategy: Eve picks encoding b_E u.a.r and measures Alice's qubit. Let $|\Psi_{ab_E}\rangle$ be the result. She sends it to Bob.

- If $b^A \neq b^B$, Bob does not check, so Eve is not detected cheating
- If $b^A = b^B$ and $b^E = b^A$, then $|\Psi_{ab^E}\rangle = |\Psi_{ab^A}\rangle$, so Eve is not detected
- If $b^A = b^B$ and $b^E \neq b^A$, then

<p>Alice</p> $ \Psi_{01}\rangle = \frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$	<p>Eve : measure in $\{ 0\rangle, 1\rangle\}$</p> <p>outcome $0\rangle$, w.p.1/2</p> <p style="padding-left: 40px;">$1\rangle$, w.p.1/2</p>	<p>Bob: measure in $\{\frac{1}{\sqrt{2}}(0\rangle \pm 1\rangle)\}$</p> <p>outcome $+\rangle$, w.p.1/2</p> <p style="padding-left: 40px;">$-\rangle$, w.p.1/2</p>
---	--	--

Unconditional Key Distribution



Proof of Security (idea)

- Eve gets information, she disturbs the state (Heisenberg)

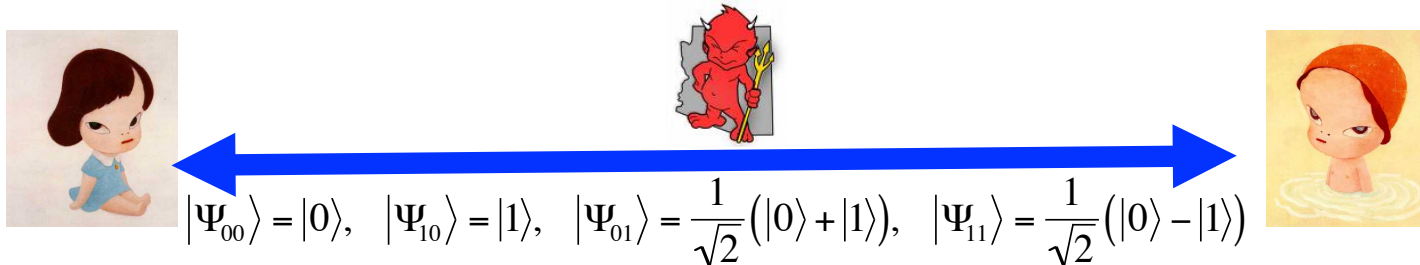
Possible strategy: Eve picks encoding b_E u.a.r and measures Alice's qubit. Let $|\Psi_{ab_E}\rangle$ be the result. She sends it to Bob.

- If $b^A \neq b^B$, Bob does not check, so Eve is not detected cheating
- If $b^A = b^B$ and $b^E = b^A$, then $|\Psi_{ab_E}\rangle = |\Psi_{ab^A}\rangle$, so Eve is not detected
- If $b^A = b^B$ and $b^E \neq b^A$ and Alice and Bob check, then

<p>Alice</p> $ \Psi_{01}\rangle = \frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$	<p>Eve : measure in $\{ 0\rangle, 1\rangle\}$</p> <p>outcome $0\rangle$, w.p.1/2</p> <p>$1\rangle$, w.p.1/2</p>	<p>Bob: measure in $\{\frac{1}{\sqrt{2}}(0\rangle \pm 1\rangle)\}$</p> <p>outcome $+\rangle$, w.p.1/2</p> <p>$-\rangle$, w.p.1/2</p>
---	--	--

Overall, $\Pr[\text{Eve is detected cheating}] = 1/16$

Unconditional Key Distribution



Proof of Security (continued)

- The optimal strategy of Eve is not much better than the one we described. (individual vs coherent attacks)
- The key is almost secure. We can distill a much stronger key by classical privacy amplification
- No assumptions on Eve's computational power!

3) Cryptography: Open Problems

- Other Cryptographic Primitives
 - Oblivious Transfer
 - Coin Flipping
 - Bit Commitment
- Practical Quantum Cryptography



- Commercial systems for QKD
- Classical cryptography secure against quantum

Outline

- 1) Introduction to the model
 - Superdense Coding
 - Teleportation

- 2) Basic algorithms
 - Deutsch-Jozsa

- 3) Cryptography
 - Key Distribution

- 4) Communication Complexity
 - Quantum fingerprints
 - Exponential Separations

4) Communication Complexity



Input x

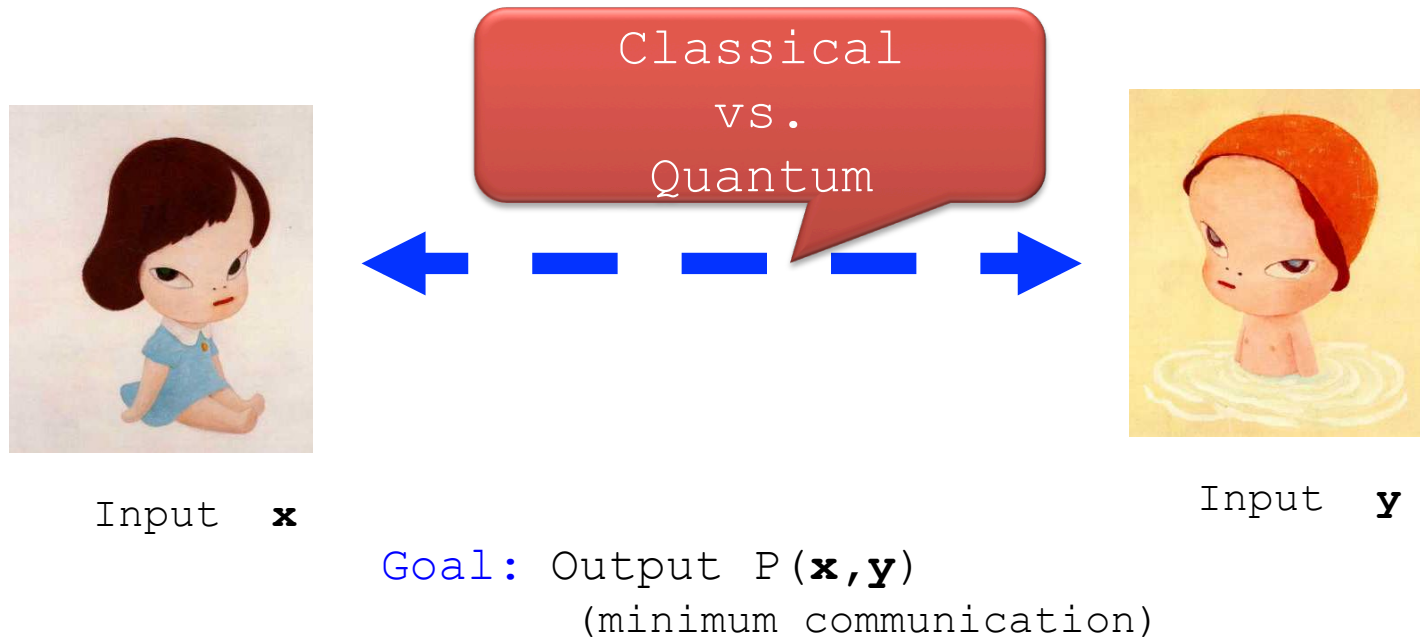


Input y

Goal: Output $P(x, y)$
(minimum communication)

- **Examples:** Is $x=y?$, Find an i such that $x_i \neq y_i$
- **Applications of Communication Complexity**
VLSI design, Boolean circuits, Data structures,
Automata, Formula size, Data streams, Secure Computation

Quantum Communication Complexity



- **Examples:** Is $x=y?$, Find an i such that $x_i \neq y_i$
- **Applications of Communication Complexity**
VLSI design, Boolean circuits, Data structures,
Automata, Formula size, Data streams, Secure Computation

Encoding Information with Quantum states

- We can encode a string $x \in \{0, 1\}^n$ with $\log n$ qubits.

$$|\phi\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^n (-1)^{x_i} |i\rangle$$

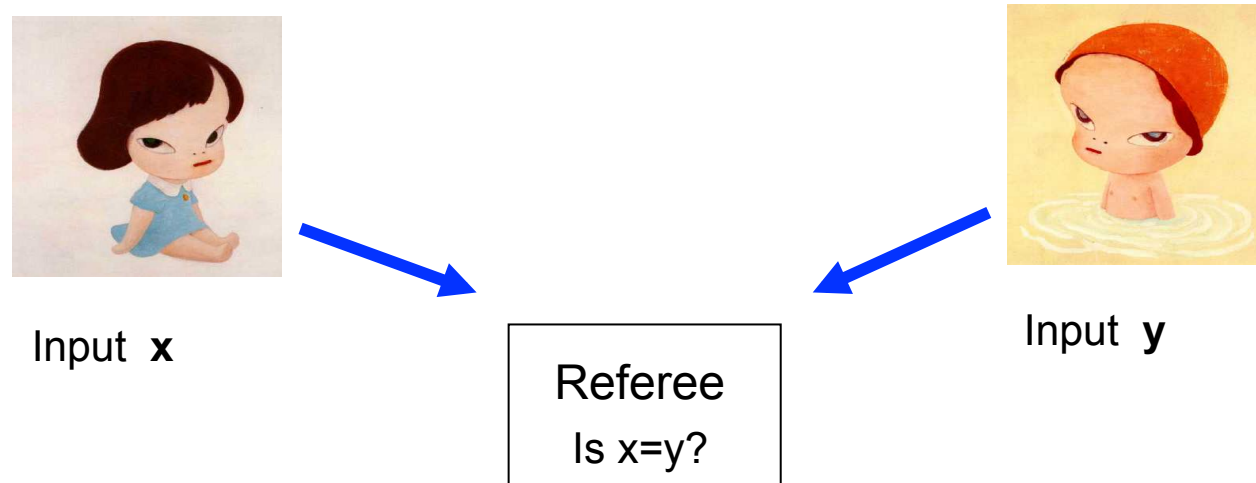
$$x = 0110$$

$$|\varphi\rangle = \frac{1}{2}(|0\rangle - |1\rangle - |2\rangle + |3\rangle)$$

$$|\varphi\rangle = \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle)$$

- Holevo's bound
 - We cannot compress information by using qubits.
We need n qubits to transmit n classical bits.
- Quantum communication can still be useful since in many communication problems the information that needs to be transmitted is small. (e.g. Equality)

Equality in Simultaneous Messages



Randomized algorithm (Complexity $O(\sqrt{n})$)

Alice and Bob use an error correcting code C with constant distance and size $O(n)$.

They each send $O(\sqrt{n})$ bits of their strings $C(x), C(y)$

Referee outputs Yes if $C(x)_i = C(y)_i$

Equality in Simultaneous Messages

Quantum algorithm : (Complexity $O(\log n)$) [BCWdW01]

- Alice and Bob use an error correcting code C with constant distance.
- They send the states

$$|\phi\rangle = \sum_{i=1}^{cn} (-1)^{C(x)_i} |i\rangle \quad |\psi\rangle = \sum_{i=1}^{cn} (-1)^{C(y)_i} |i\rangle$$

- Referee measures the state $|\phi\rangle \otimes |\psi\rangle$

in the symmetric and alternating subspace of $\mathcal{R}^n \otimes \mathcal{R}^n$

- If $x=y$, then the states are equal.
- If $x \neq y$, then the states are almost orthogonal.

Exponential Separations

- Two-way communication
 - [BCW98]: exponential separation for zero error.
 - [Raz99]: exponential separation for bounded error.
 - [Gav07, RK11]: between q . One-way and rand. Two-way
- One-way communication
 - [BJK04]: exponential separation for a relation
 - [GKKRdW07]: exponential separation for a partial function
- Simultaneous Messages
 - [BCWdW01]: equality via fingerprints
 - [BJK04]: exponential separation for a relation

The Hidden Matching Problem



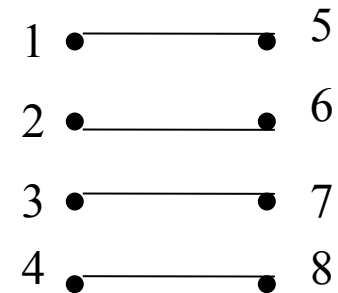
Input: $x \in \{0,1\}^{2n}$

Input: a matching M on $[2n]$

Output:

$((i, j), x_i \oplus x_j),$
for $(i, j) \in M$

eg. $\{(1, 5), (2, 6), (3, 7), (4, 8)\}$



Theorem

- There exists a one-way quantum protocol with compl. $O(\log n)$
- Any randomized one-way protocol has complexity $\Omega(\sqrt{n})$

Quantum algorithm for HM_4

Let $M = \{(1,3), (2,4)\}$ be Bob's matching.

- Alice sends the state

$$\frac{1}{2}((-1)^{x_1}|1\rangle + (-1)^{x_2}|2\rangle + (-1)^{x_3}|3\rangle + (-1)^{x_4}|4\rangle)$$

$x = 0011$
$ 1\rangle + 2\rangle - 3\rangle - 4\rangle$

- Bob measures in the basis $B = \{|1\rangle + |3\rangle, |1\rangle - |3\rangle, |2\rangle + |4\rangle, |2\rangle - |4\rangle\}$

$$\text{and outputs } \left\{ \begin{array}{ll} ((1, 3), 0) & \text{if he measures } |1\rangle + |3\rangle \\ ((1, 3), 1) & \text{" } |1\rangle - |3\rangle \\ ((2, 4), 0) & \text{" } |2\rangle + |4\rangle \\ ((2, 4), 1) & \text{" } |2\rangle - |4\rangle \end{array} \right.$$

Quantum algorithm for HM₄

- Alice sends the state

$$\frac{1}{2} \sum_{i=1}^4 (-1)^{x_i} |i\rangle = \frac{1}{2} ((-1)^{x_1} |1\rangle + (-1)^{x_3} |3\rangle) + \frac{1}{2} ((-1)^{x_2} |2\rangle + (-1)^{x_4} |4\rangle)$$

- Bob measures in the basis

$$B = \{|1\rangle + |3\rangle, |1\rangle - |3\rangle, |2\rangle + |4\rangle, |2\rangle - |4\rangle\}$$

- $\Pr[\textit{outcome } |1\rangle + |3\rangle] = \frac{1}{8} ((-1)^{x_1} + (-1)^{x_3})^2$

$$\Pr[\textit{outcome } |1\rangle - |3\rangle] = \frac{1}{8} ((-1)^{x_1} - (-1)^{x_3})^2$$

- Bob can compute the XOR of a pair of the matching with probability 1.

4) Communication Complexity

Open Problems

- Quantum communication complexity of **total functions**
- Power of **entanglement** in communication complexity
- Communication Complexity with **super-quantum** resources.

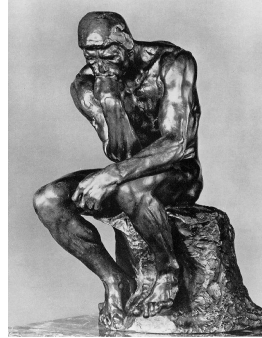
Conclusions

Quantum Information can be very powerful

- Algorithms
 - Factoring, Unordered Search
 - Quantum Walks, etc
- Communication Complexity
 - Many exponential separations
 - Total Functions
- Cryptography
 - Unconditional Key Distribution
 - Impossibility of Bit Commitment, OT
- Interactions with Complexity Theory & Physics
 - Ronald's talk

Why is Quantum
Computation
important?

Further Conclusions



- Quantum Information and Computation
 - Computational power of nature
 - Quantum Mechanics as an theory of information
 - Advances in classical Computer Science
 - Practical Quantum Cryptography
 - Advances in Experimental Physics

Simon's Algorithm

Let $f: \{0,1\}^n \rightarrow \{0,1\}^n$

Promise: $f(x)=f(x+a)$ and $f(x) \neq f(y)$, $y \neq x+a$ (2-periodic)

Goal: Find a

Randomized: $2^{n/2}$

Quantum: $O(n)$, by finding each time a random y , st. $y \cdot a = 0$

$$\begin{aligned}
 |0\dots 0\rangle|0\dots 0\rangle &\xrightarrow{H \text{ on } 1st} \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle|0\dots 0\rangle \xrightarrow{O_f} \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle|f(x)\rangle \\
 &\xrightarrow{\text{measure } f(x)} \frac{1}{\sqrt{2}} |x\rangle + \frac{1}{\sqrt{2}} |x+a\rangle \xrightarrow{H} \frac{1}{2^{n+1/2}} \sum_{y \in \{0,1\}^n} (-1)^{xy} |y\rangle + \frac{1}{2^{n+1/2}} \sum_{y \in \{0,1\}^n} (-1)^{(x+a)y} |y\rangle
 \end{aligned}$$

$$\text{amplitude of } |y\rangle = \frac{1}{2^{n+1/2}} (-1)^{xy} + \frac{1}{2^{n+1/2}} (-1)^{(x+a)y} = \frac{1}{2^{n+1/2}} (-1)^{xy} [1 + (-1)^{ay}]$$

Hence, we only measure y , s.t. $a \cdot y = 0$

Repeat $O(n)$ times to get n linear independent y 's.

Period Finding Algorithm

Let $f: \mathbb{Z}_N \rightarrow \mathbb{C}$

Let $f: \mathbb{Z}_N \rightarrow \mathbb{C}$

Promise: f is periodic

Goal: Find period

Tool: Quantum Fourier Transform: $|x\rangle \xrightarrow{QFT_N} \frac{1}{\sqrt{N}} \sum_{y \in \{0,1\}^n} \omega^{xy} |y\rangle$, $\omega = e^{2\pi i/N}$

$$|0\dots 0\rangle|0\dots 0\rangle \xrightarrow{QFT_N \text{ on } 1st} \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} |x\rangle|0\dots 0\rangle \xrightarrow{O_f} \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} |x\rangle|f(x)\rangle$$

$$\xrightarrow{\text{measure } f(x)} \frac{1}{\sqrt{N/r}} \sum_{j=0}^{N/r-1} |j \cdot r + l\rangle \xrightarrow{QFT_N} \frac{1}{\sqrt{r}} \sum_{i=0}^{r-1} |i \cdot N/r\rangle$$

$$\xrightarrow{\text{measure}} |k \cdot N/r\rangle, \quad k \in [0, r-1]$$

If $\gcd(k, r) = 1$, then $\gcd(kN/r, N) = N/r$

REMARK: Factoring reduces classically to period finding!!!