CS290A, Spring 2005:

Quantum Information & Quantum Computation

Wim van Dam

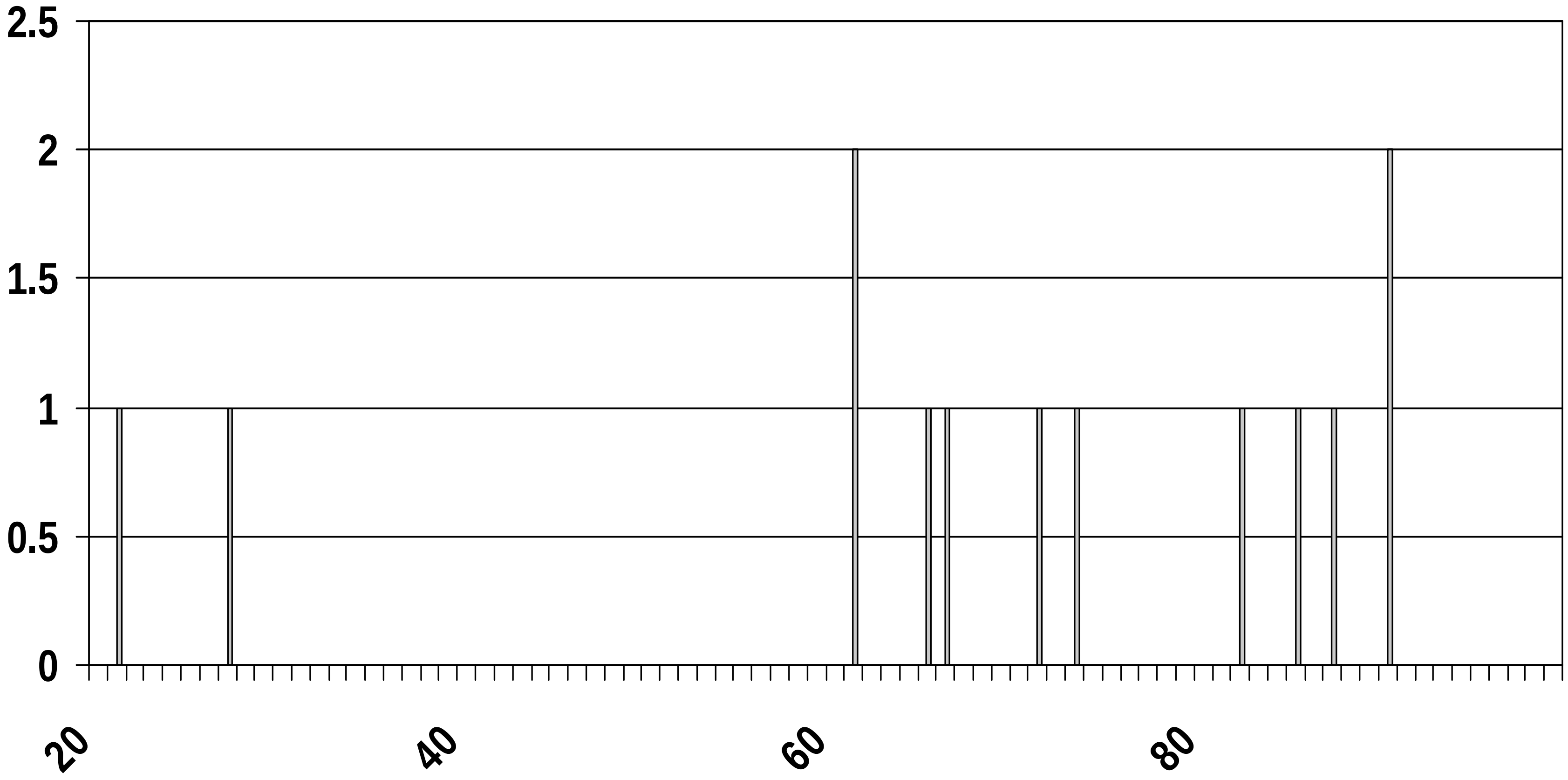
Engineering 1, Room 5109
vandam@cs

http://www.cs.ucsb.edu/~vandam/teaching/CS290/

Administrivia

- Comprehensive exams will be *closed* book.
- Final exam will be *open* book.
- Small correction to Midterm scores:

Midterm Scores



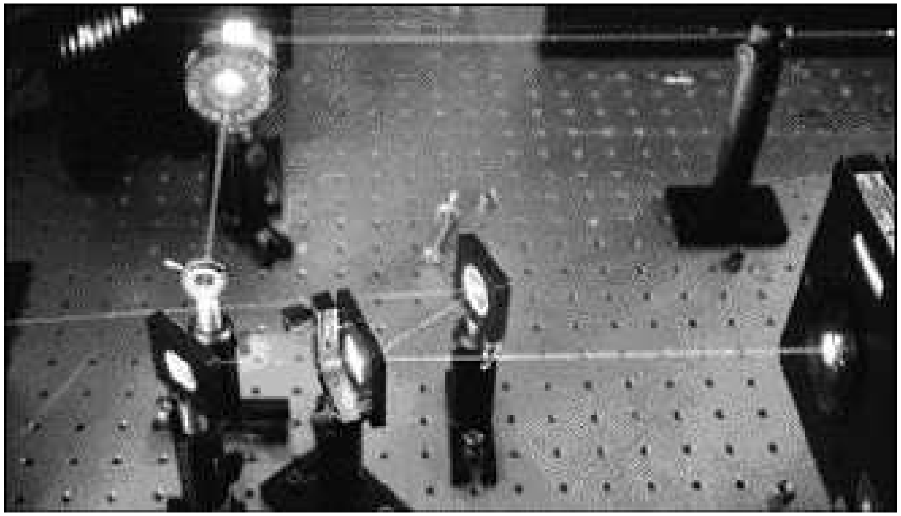
Total number of grades: 13

Beyond Quantum Algorithms

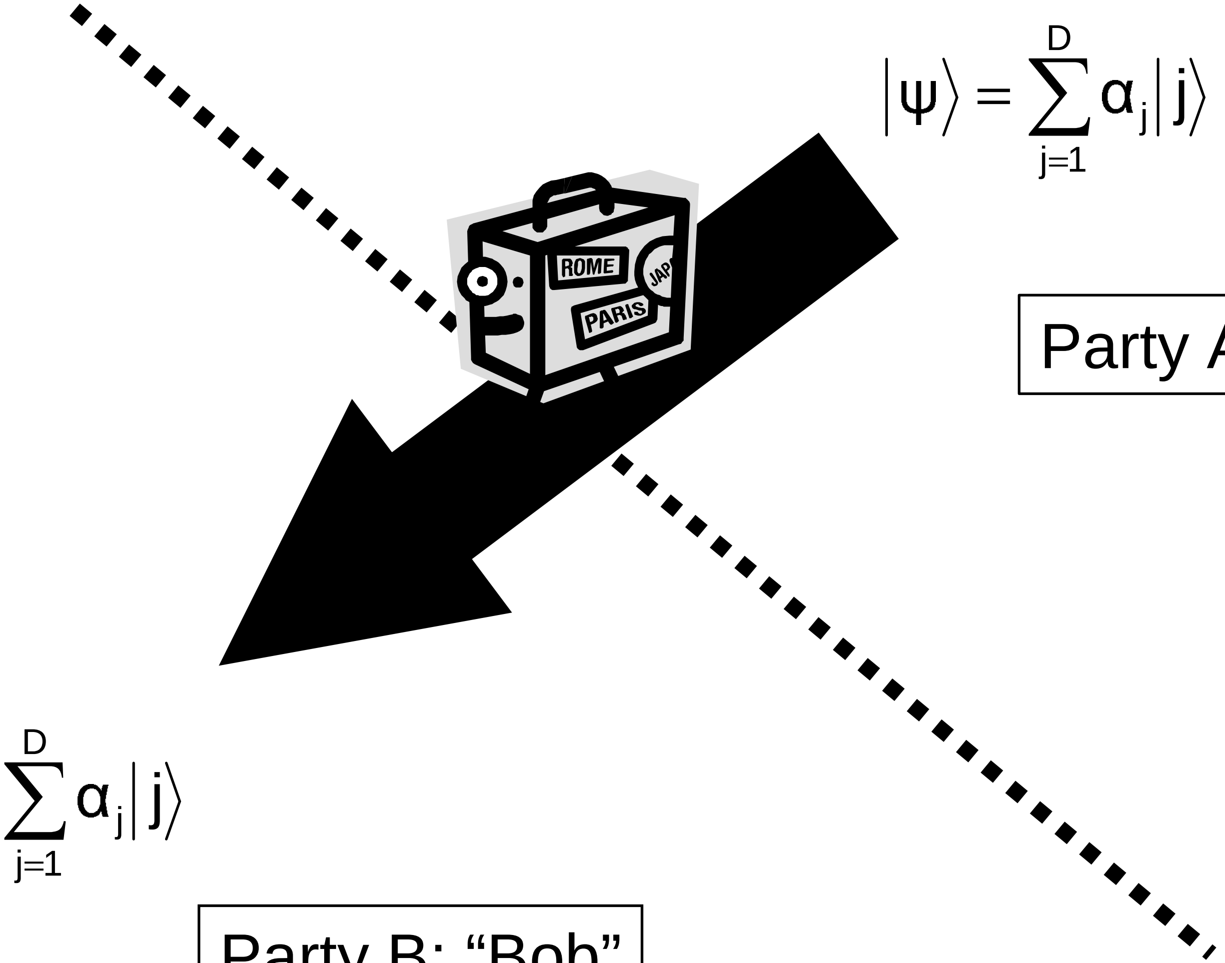
The remaining weeks we will look at non-algorithmic applications of quantum information theory :

- Quantum cryptography
- Quantum communication theory/distributed computing
- Superdense coding/Teleportation

These protocols require only a few qubits and are therefore much easier to implement experimentally (using photons).



Quantum Communication



$$\left|\psi\right\rangle = \sum_{j=1}^{D} \alpha_j \left|j\right\rangle$$

Party A: “Alice”

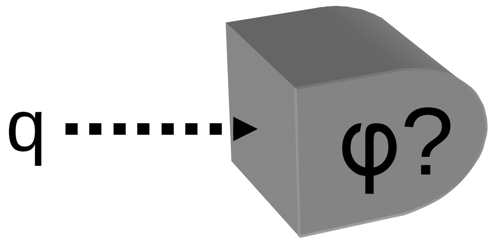
$$\left|\psi\right\rangle = \sum_{j=1}^{D} \alpha_j \left|j\right\rangle$$

Party B: “Bob”

How Much Classical Information in One Qubit?

- A qubit $|q\rangle = \alpha|0\rangle+\beta|1\rangle$ has to be described by two complex values $\alpha,\beta \in \mathbb{C}$.
- Suggests the (unreasonable) amount of ∞ bits of classical information stored in a single qubit.
- This is not the case. Holevo’s bound:
  One qubit can only carry only one bit of information

Measuring a Qubit



The measurement device can 'ask' if $\left|q\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$ equals the state $\left|\varphi\right\rangle = \gamma\left|0\right\rangle + \delta\left|1\right\rangle$.

$$\boxed{\Pr(\varphi|q) \quad = \quad \left\langle\varphi|q\right\rangle\left\langle q|\varphi\right\rangle \quad = \quad \left|\alpha\overline{\gamma} + \beta\overline{\delta}\right|^2}$$

We implement this measurement with the use of the unitary transformation M:$|\varphi\rangle \mapsto |0\rangle$ and M:$|\varphi^\perp\rangle \mapsto |1\rangle$.

Terminology: "We measure $|q\rangle$ in the $\{|\varphi\rangle,|\varphi^\perp\rangle\}$ basis."

Disturbing Measurements

- Measuring the qubit $|q\rangle = \alpha|0\rangle+\beta|1\rangle$ in the 0/1 basis gives only a rough indication of the values $|\alpha|^2$ and $|\beta|^2$.

- After the measurement, the qubit has collapsed to either zero or one, and does not contain any information about α and β anymore.

- A second copy of $|q\rangle$ would tell us more.

One, Two, Many Qubits

- To determine the amplitudes of an unknown qubit we need an unlimited supply of fresh copies of it.

- More precisely, k copies of $|q\rangle = \alpha|0\rangle+\beta|1\rangle$ will give us approximately log(k+1) bits of information about the amplitudes α and β.

“Knowing a qubit”* equals *“having an infinity supply of them”* equals *“having a device that produces them at will”.

No-Cloning Theorem

- Imagine a quantum mechanical process that would implement the following evolution: $|q,\_\rangle \mapsto |q,q\rangle$
- This contradicts the unitary/linearity restriction of quantum physics.

It is impossible to make a device that perfectly copies an unknown qubit.

Two Qubit Bases

Define the four qubit states:

Both {0,1} and {+,–} form an orthogonal qubit basis.

$$\left\{\begin{array}{lcl} |0\rangle & & \\ |1\rangle & & \\ |+\rangle & = & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |-\rangle & = & \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{array}\right.$$

The sources

prob.:	state:
$\frac{1}{2}$	$\|0\rangle$
$\frac{1}{2}$	$\|1\rangle$

and

prob.:	state:
$\frac{1}{2}$	$\|+\rangle$
$\frac{1}{2}$	$\|-\rangle$

are indistinguishable from each other.

Wiesner’s Quantum Money

- A quantum bill contains a serial number N, and 20 random qubits from the set {0,1,+,–}.

- The National Bank knows which string $\{0,1,+,–\}^{20}$ is associated with which N.

- The Bank can check the validity of a bill N by measuring the qubits in the proper 0/1 or +/– bases.

- A counterfeiter cannot copy the bill if he does not know the 20 bases of the qubits.

Security of Quantum Money

Not knowing the right basis, it is impossible to copy the quantum code.

Measuring the code in the wrong basis, destroys the quantum code in an irreversible way.

Informal mathematical argument:

a) 40 bits of information are required to reproduce the quantum code perfectly.
b) Holevo’s bound: the 20 qubits will only give 20 bits of information.
c) Probability of being successful in copying the 20 qubits is $(3/4)^{20}$.

A Failed Attempt

- If the forger is facing 20 unknown qubits $\{0,1,+,–\}^{20}$

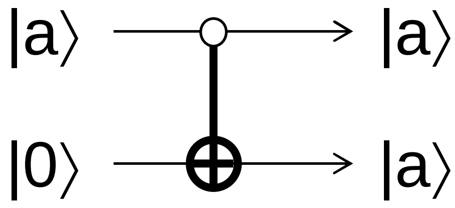
- Attempt #1: Measure in a random basis {0,1} or {+,–} and copy the result to a new bill.
- Success rate per bit: ¾; total success rate $(¾)^{20} \approx 0.3\%$
- The probability per bit of getting detected is ¼.

- The answer to Exercises II, Question 4 shows that it is impossible to copy the unknown qubit values {0,1,+,–}.

- Can we wait with measuring the qubit and fool the bank first before copying the money. A CNOT maybe?

A more Elaborate Failure

- Attempt #2: Take the unknown qubit {0,1,+,–}, apply a CNOT to it and a state |0〉, send the original qubit to the bank, let the bank check it, then proceed with the copy.



goes to bank who will check value

goes to forger…

- The CNOT copy gives:

$$\left|0\right\rangle \mapsto \left|0{,}0\right\rangle \qquad \left|+\right\rangle \mapsto \frac{1}{\sqrt{2}}(\left|0{,}0\right\rangle + \left|1{,}1\right\rangle)$$

$$\left|1\right\rangle \mapsto \left|1{,}1\right\rangle \qquad \left|-\right\rangle \mapsto \frac{1}{\sqrt{2}}(\left|0{,}0\right\rangle - \left|1{,}1\right\rangle)$$

- This works fine for the {0,1} basis, but what about +/–?

Measuring Entangled States

- Assume that the value was +, such that after the CNOT we have the non-tensor product state $(|00\rangle+|11\rangle)/\sqrt{2}$.
- What will the bank see when it measures its bit in the assumed basis {+,–}? See Handout III.
- Note: $\frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle) = \frac{1}{\sqrt{2}}(|+,+\rangle + |-,-\rangle)$
- Hence the bank will observe a random value + or –; with 50% chance the bank will detect that the bit has been tampered with. Total failure rate is again ¼.

Quantum Cryptography

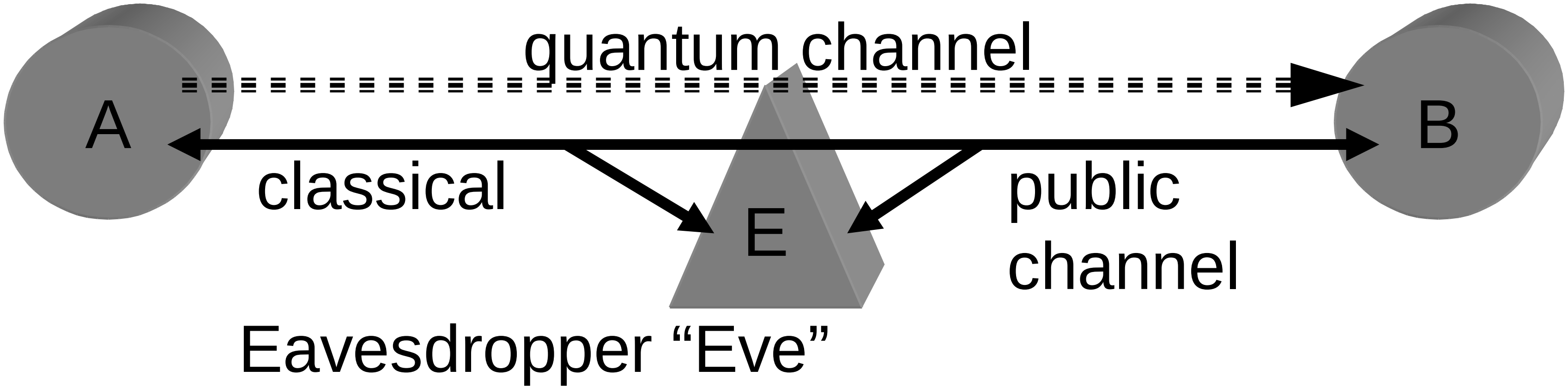
- In 1984 Bennett and Brassard described how the quantum money idea with its basis {0,1} vs. {+,–} can be used to implement a quantum key distribution protocol that is unbreakable by the laws of quantum mechanics.
- This so-called **BB84** protocol has very modest requirements from an experimental point-of-view: single qubits and single qubit measurements.
- Implementations of this protocol are commercially available.

BB84 Cryptography

Central idea: Quantum Key Distribution (QKD) via the {0,1,+,–} states between Alice and Bob.

Security is guaranteed by the rule: “Information gain implies state disturbance”, which will apply to the eavesdropper Eve.

O(N) classical and quantum communication to establish N shared key bits.



BB84 Protocol

1) Alice sends 4N random qubits ∈ {0,1,+,–} to Bob.

2) Bob measures each qubit in 0/1 or +/– basis.
(The choice of basis is made randomly.)

quantum

3) Alice and Bob announce their respective 4N bases.
They continue with the ~2N outcomes for which the same basis was used.

Classical & Public

4) Alice and Bob verify measurement outcomes on random (size N) subset of the 2N bits.

5) Remaining N outcomes function as secret key.

shared

One Time Pad Encryption

- Standard:
  If Alice and Bob share N random bits $b_1,\ldots,b_N \in \{0,1\}^N$
  then A can encrypt her secret message $m_1,\ldots,m_N \in \{0,1\}^N$
  by sending to Bob the encrypted string $b_1 \oplus m_1,\ldots,b_N \oplus m_N$.

- Bob decrypts the message by using the shared m_j bits in the equation $(m_j \oplus b_j) \oplus b_j = m_j$ for all the N bits.

- As long as b is unknown, this is absolutely secure.

Security of BB84

Not knowing the proper basis, Eve cannot
- copy the qubits that are passing by,
- measure the states without disturbing them.

Any serious attempt by Eve will be detected by Alice and Bob when they the perform the ‘equality check’ on half of their shared random bits.

The final N shared, random bits can be used for Vernam-like encryption of an N bits message. (XOR-ing the message with the random bits.)

Practical Feasibility of QKD

Only single qubits are involved.

Simple state preparations and measurements.

No ‘qubit storage’ necessary, only communication.

Realizable with ‘photon polarization’.

(Imperfect states, channels and measurements can be dealt with, without giving up above advantages.)

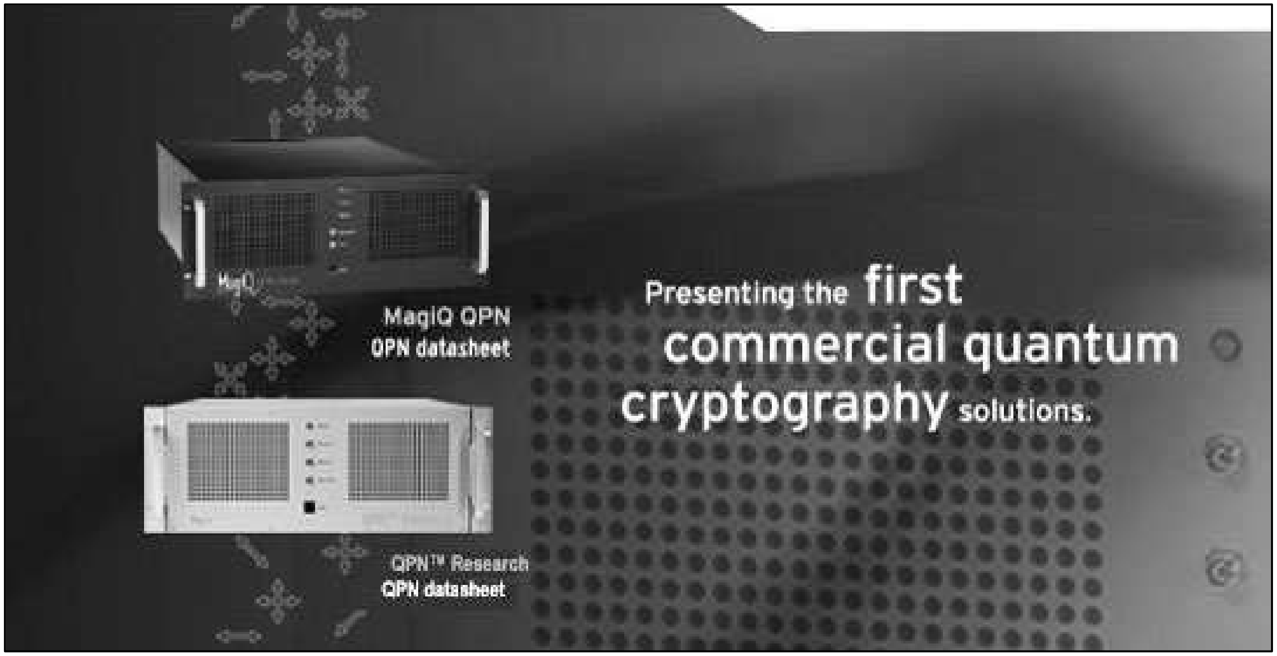
Arguments Against QKD

QKD is not public key cryptography;
it ***does not*** *"fix what Peter Shor broke".*

Expensive for long keys: Ω(N) qubits of communication for a key of size N.

Eve can sabotage the quantum channel, thereby forcing Alice and Bob to use classical cryptography after all.

Commercial Availability…



Presenting the first commercial quantum cryptography solutions.

Entanglement

- The security of quantum money and BB84 against CNOT copying relies on the behavior of $(|00\rangle+|11\rangle)/\sqrt{2}$.

- This state is an example of an entangled state that can not be written as a tensor product $|x\rangle\otimes|y\rangle$.

- This entanglement is the source of a lot of non-classical properties of (distributed) quantum bits.

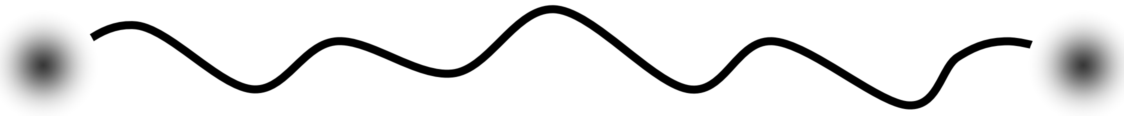
More on Entanglement

The state (|00⟩+|11⟩)/√2 is called an “EPR pair” after Einstein, Podolsky, Rosen who introduced it.

How does the state behave when it is distributed over two different places A and B?

$$\frac{1}{\sqrt{2}}\left(\begin{array}{c} \left|0_A \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots 0_B\right\rangle \\ + \\ \left|1_A \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots 1_B\right\rangle \end{array}\right)$$

The two qubits will behave in an entangled way that is uniquely quantum mechanical.



Some EPR Observations

- If Alice measure in the {0,1} basis then she will observe a random outcome. If, afterwards Bob measures in the same {0,1} basis, he will measure the same value.

- If Alice measure in the {+,–} basis then she will observe a random outcome. If, afterwards Bob measures in the same {+,–} basis, he will measure the same value.

- If Bob measure in the {0,1} basis then he will observe a random outcome. If, afterwards Alice measures in the same {0,1} basis, she will measure the same value.

- And so on…

More EPR Observations

- It does not matter in which basis $\{|\varphi\rangle,|\varphi^{\perp}\rangle\}$ Alice/Bob measures her/his part of the entangled qubits:
  the outcome will always be completely random.

- It does not matter who goes first: what A does on her side will not affect B’s statistics and vice versa.
- (Special relativity tells us that with large distances and small time intervals one cannot say who acts ‘first’.)

- However, it is the case that the outcomes will be correlated: If A measures a 0, then B will so too, etc.