MINO

Quantum computing and networking
Lecture 3: Communication protocols that use a few Qbits

Philippe Nain (Inria emeritus)

Quantum Computer Science – An introductio

by N. David Mermin

Cambridge University Press, 2007

Chapter 6

Communication protocols that use a few Qbits

- Quantum cryptography
  - BB84 protocol
  - E91 protocol
- Quantum dense coding
- Quantum teleportation

Communication protocols that use a few Qbits

As an easy start let us watch short video setting up the stage …

https://www.youtube.com/watch?v=hRFQd_fkzws

Quick reminder (see lectures 1 & 2)

A **Qbit** (or qubit, qbit, q-bit) is a quantum mechanical system which under some suitable circumstances can be treated as having only two quantum levels.

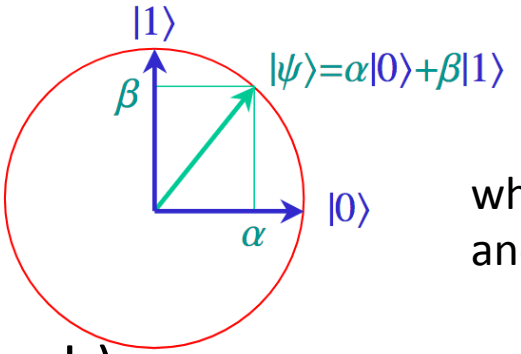
You can use it to encode quantum information, in a similar way as you would in a classical computer when you encode information in the two possible states, **on** or **off**, of a transistor.

Quick reminder (see lectures 1 & 2)

State of a Qbit: unit vector in 2D complex vector space

$|\psi> = \alpha|0> + \beta|1>$ with α and β complex numbers, called amplitudes,

satisfying $|\alpha|^2 + |\beta|^2 = 1$ with $|0> = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1> = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$



when α and β re
and $\alpha^2 + \beta^2 = 1$

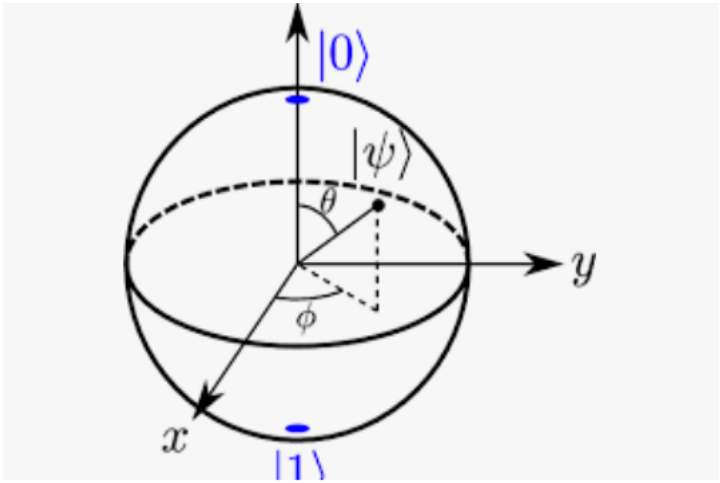
3D representation: Bloch sphere (named after Felix Bloch)

In this representation

$|0> = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ and $|1> = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}$, north and south poles

θ, φ give the unique point (x,y,z)

with $x = \sin(\theta)\cos(\varphi), y = \sin(\theta)\sin(\varphi), z = \cos(\theta)$



Quick reminder (see lectures 1 & 2)

A Qbit can be in both states |0> and |1> « at the same time » (not satisfactory explanation → open problem in physics).

When state of Qbit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is measured, we find

- $|0\rangle$ with prob. $|\alpha|^2$; after measurement $|\psi\rangle = |0\rangle$
- $|1\rangle$ with prob. $|\beta|^2$; after measurement $|\psi\rangle = |1\rangle$

→ Quantum state collapses after measurement.

Quick reminder (see lectures 1 & 2)

$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ called "ket 0", $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ called "ket 1", named by Paul Dirac in 1939

$|0\rangle, |1\rangle$ orthonormal basis -- called "computational basis"

Three important unitary transformations

Unitary matrix

set of complex numbers.

natrix transformation **U**: $C^n \longrightarrow C^n$ is **unitary** if the conjugate transpose of **U** is also its inverse, namely, **UU*** = **U*U** = **I**, with **I** the identity trix.

perties:

given x and y complex vectors in C^n, multiplication by **U** preserves their inner product, that is, <**U**x, **U**y> = <x,y>. In particular, lengths (||**U**x|| =||x||) and angle between vectors are preserved

columns of **U** form orthonormal basis of C^n wrt usual inner product

if x and y are unit vectors (i.e. ||x||=||y||=1) there exists unitary matrix **U** such that **U** x = y.

Quick reminder (see lectures 1 & 2)

$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ called "ket 0", $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$ called "ket 1", named by Paul Dirac in 1939

$|0\rangle, |1\rangle$ orthonormal basis -- called "computational basis"

Three important unitary transformations

$\Rightarrow H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$ Hadamard gate ; $H^2 = I$ (Identity matrix)

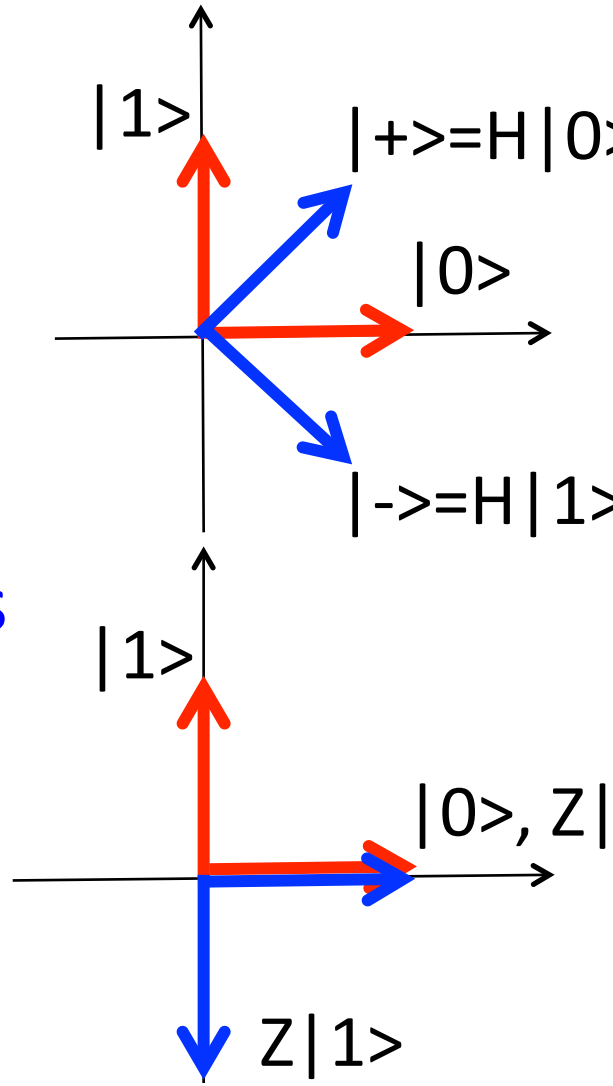
$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) := |+\rangle, \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) := |-\rangle$

H, X, Z reversible transformations

$|+\rangle, |-\rangle$ another useful orthonormal basis

$\Rightarrow X = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}, \quad X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle ; \quad X^2 = I$

$\Rightarrow Z = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}, \quad Z|0\rangle = |0\rangle, \quad Z|1\rangle = -|1\rangle ; \quad Z^2 = I$



Quick reminder (see lectures 1 & 2)

A single Qbit « lives » in vector space C^2.

More generally, a system with n Qbits – referred to as n-Qbit – « lives » in vector space C^m with $m = 2^n$.

E.g. a 2-Qbit can be in any superposition

$$\alpha_0 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \alpha_1 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \alpha_2 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \alpha_3 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \alpha_0 |00> + \alpha_1 |01> + \alpha_2 |10> + \alpha_3 |11>, \quad \text{with} \sum_{i=0}^{3} |\alpha_i|^2 = 1.$$

By convention $|ab> = |a> \otimes |b>$ with $\otimes$ tensor product.

Quick reminder (seee lectures 1 & 2)

Qbits ψ_1 and ψ_2 are entangled (correlated) if state of their superposition does not take product form $|\psi_1> \otimes |\psi_2>$.

For instance, consider 2-Qbit $\frac{1}{\sqrt{2}}(|00> + |11>$.

If one Qbit is measured in state |0> (prob. ½) other one in state |0>.
If one Qbit is measured in state |1> (prob. ½) other one in state |1>.

Both Qbits are entangled.

Quick reminder (seee lectures 1 & 2)

Proof. Assume there exist coefficients α_1, β_1, α_2, β_2 such that

$$\frac{1}{\sqrt{2}}(|00> + |11>) = (\alpha_1 |0> + \beta_1 |1>) \otimes (\alpha_2 |0> + \beta_2 |1>)$$

$$= \alpha_1\alpha_2 |00> + \alpha_1\beta_2 |01> + \beta_1\alpha_2 |10> + \beta_1\beta_2 |11> .$$

For this identity to hold, we need $\alpha_1\beta_2 = 0$ and $\alpha_2\beta_1 = 0$.
Depending on the 4 possible values for coefficients, r.h.s is either 0, 0, $\alpha_1\alpha_2|0>$, or $\beta_1\beta_2|1>$. Equality cannot hold.

Therefore $\frac{1}{\sqrt{2}}(|00> + |11>$ is not tensor product → Qbits entangled.

Quick reminder (seee lectures 1 & 2)

Measurement

- Measuring |0> in basis |0>,|1> gives classical bit 0 with prob. 1
- Measuring |1> in basis |0>,|1> gives classical bit 1 with prob. 1

- Measuring |+> = (|0>+|1>)/√2 in basis |0>,|1> gives classical bit 0 with prob. ½ and classical bit 1 with prob. ½
- Measuring |-> = (|0>-|1>)/√2 in basis |0>,|1> gives classical bit 0 with prob. ½ and classical bit 1 with prob. ½

Communication protocols that use a few Qbits

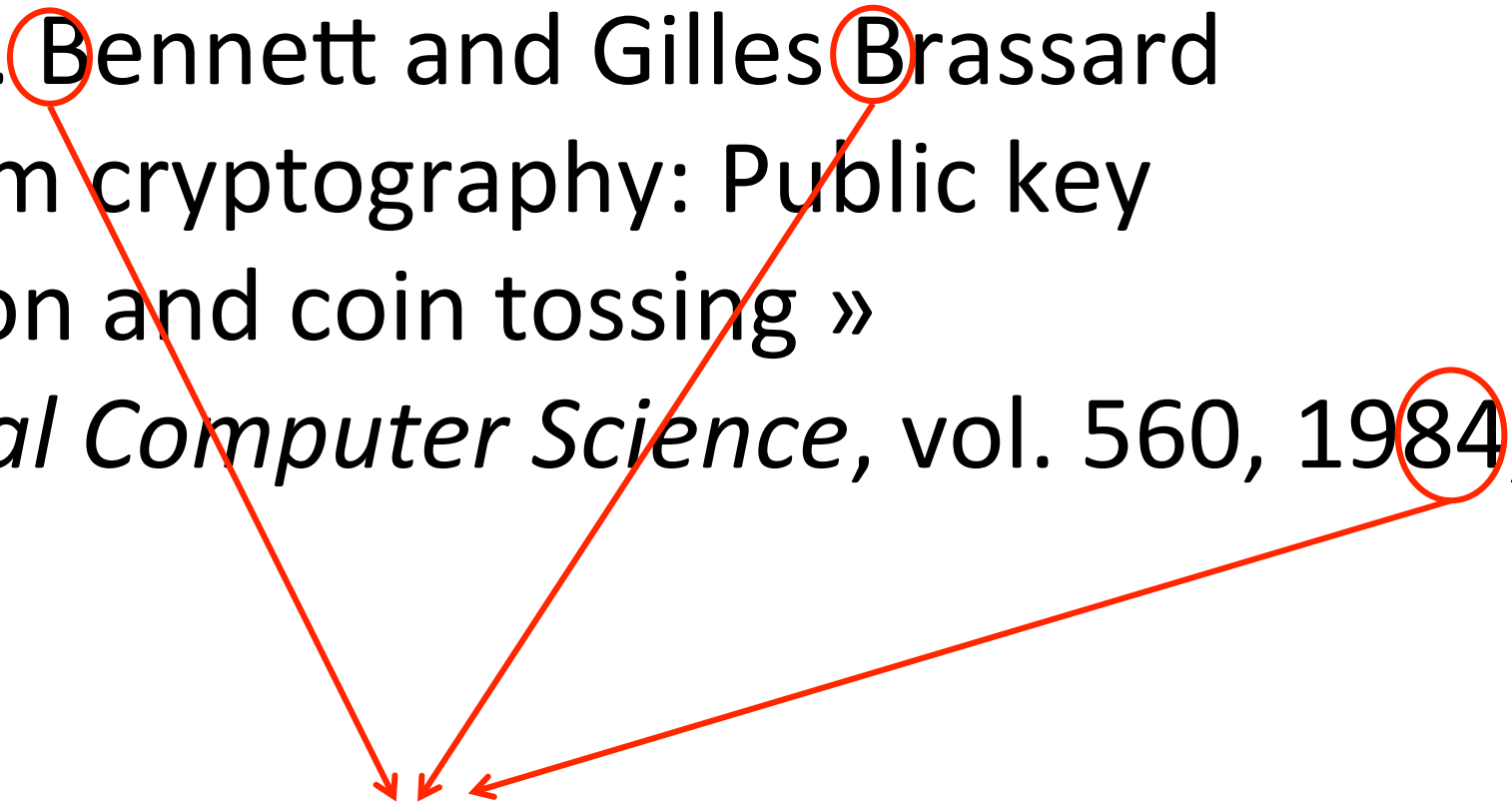
- Quantum cryptography
  - BB84 protocol
  - E91 protocol
- Quantum dense coding
- Quantum teleportation

Quantum cryptography: BB84 protocol

Charles H. Bennett and Gilles Brassard
« Quantum cryptography: Public key distribution and coin tossing »
Theoretical Computer Science, vol. 560, 1984, pp. 7–11.

Quantum cryptography: BB84 protocol

Charles H. Bennett and Gilles Brassard
« Quantum cryptography: Public key distribution and coin tossing »
Theoretical Computer Science, vol. 560, 1984, pp. 7–11.



BB84

Quantum Key Distribution (QKD)

Goal: Create shared secret key between two distant parties, Alice and Bob.

A **shared secret key** is used by mutual agreement between a sender and a receiver for encryption, decryption, and digital signature purposes.

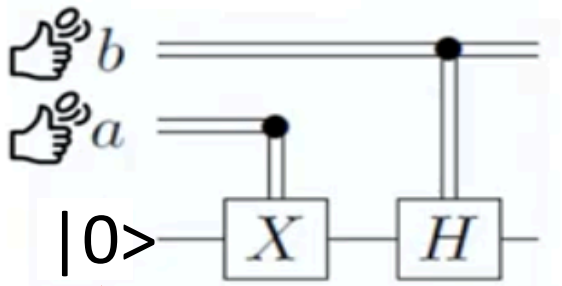
Quantum Key Distribution (QKD)

In short: if Bob possesses Alice's secret key, he can decrypt information contained in encrypted message transmitted to him by Alice.

E.g. Trivial key = « all letters in the alphabet shifted by 3 » (A→D, B→E, etc.)

BB84 protocol

Alice



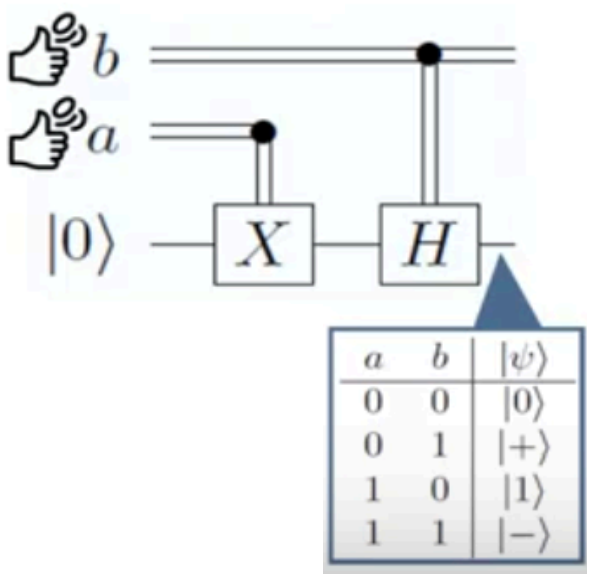
Qbit initialized in state |0>

BB84 protocol

=0 (no X), b=0 (no H)

Ψ>= |0>

Alice



a=1 (X), b=0 (no H)

X|0>=|1>

|Ψ>= |1>

=0 (no X), b=1 (H)

|0>=(|0>+|1>)/√2:=|+>

ψ> =|+>

a=1 (X), b=1 (H)

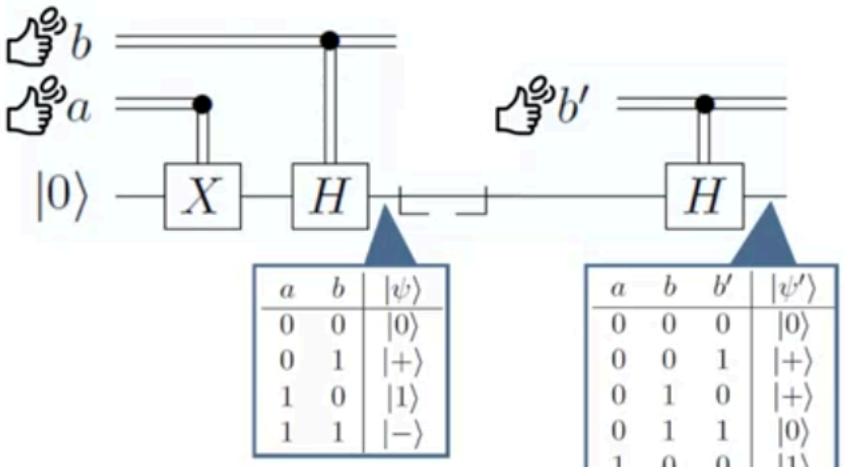
X|0>=|1>

H|1>=(|0>-|1>)/√2:=|->

|ψ> = |->

BB84 protocol

Alice Bob



a	b	$\|\psi\rangle$
0	0	$\|0\rangle$
0	1	$\|+\rangle$
1	0	$\|1\rangle$
1	1	$\|-\rangle$

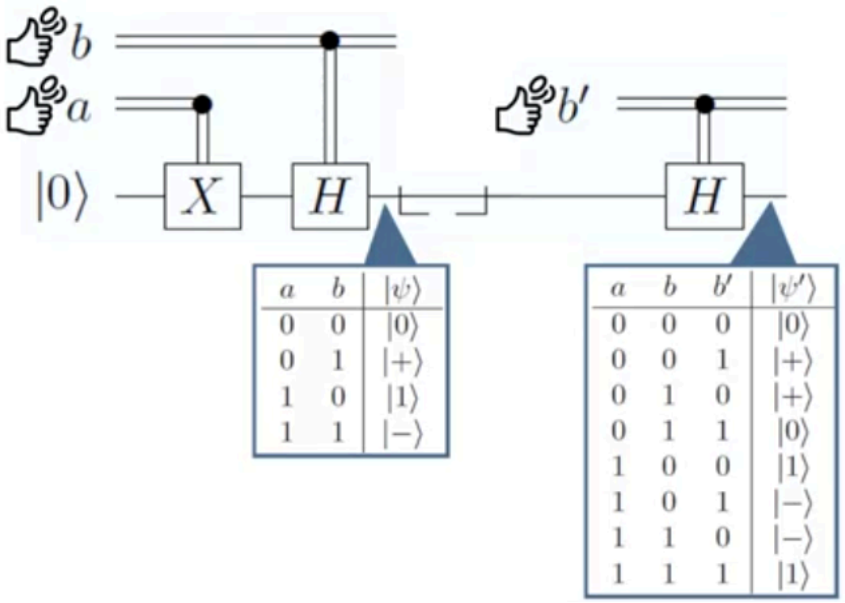
a	b	b'	$\|\psi'\rangle$
0	0	0	$\|0\rangle$
0	0	1	$\|+\rangle$
0	1	0	$\|+\rangle$
0	1	1	$\|0\rangle$
1	0	0	$\|1\rangle$
1	0	1	$\|-\rangle$
1	1	0	$\|-\rangle$
1	1	1	$\|1\rangle$

BB84 protocol

’=0 (no H)

ψ’>=|ψ>

Alice Bob



a	b	|ψ⟩
0	0	|0⟩
0	1	|+⟩
1	0	|1⟩
1	1	|−⟩

a	b	b′	|ψ′⟩
0	0	0	|0⟩
0	0	1	|+⟩
0	1	0	|+⟩
0	1	1	|0⟩
1	0	0	|1⟩
1	0	1	|−⟩
1	1	0	|−⟩
1	1	1	|1⟩

b’=1 (H), |ψ'>=H|ψ>

a=0, b=0
|ψ’>=H|0>=|+>

a=0, b=1
|ψ’>=H|+>=|0>

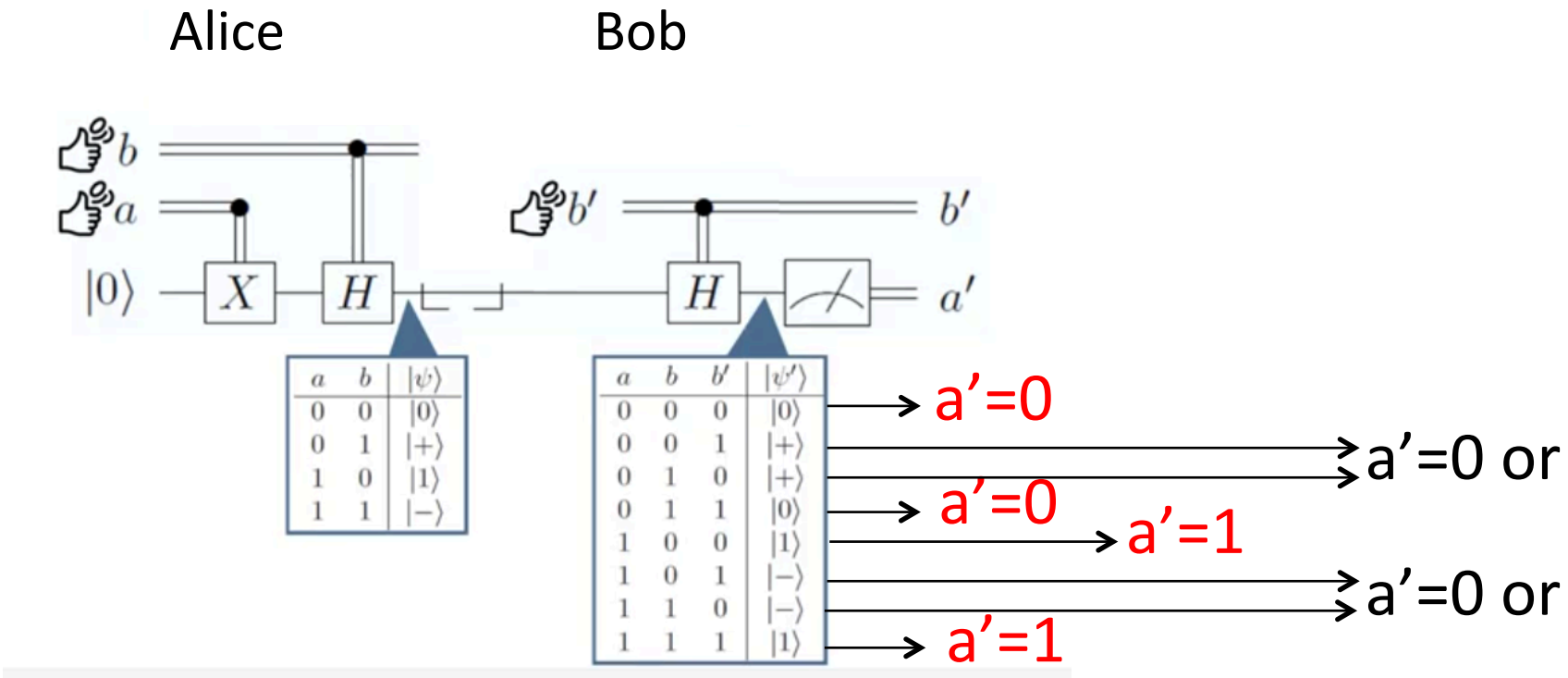
a=1, b=0
|ψ’>=H|1>=|->

a=1, b=1
|ψ’>=H|->=|1>

BB84 protocol

Now, Bob measures |ψ'> in the <u>computational basis</u> |0>, |1>

- When |ψ'>=|0> then a'=0 and when |ψ'>=|1> then a'=1
- When |ψ'>=|+> (resp. |ψ'>=|->) then a'=0 with prob. ½ and a'=1 with prob. ½.



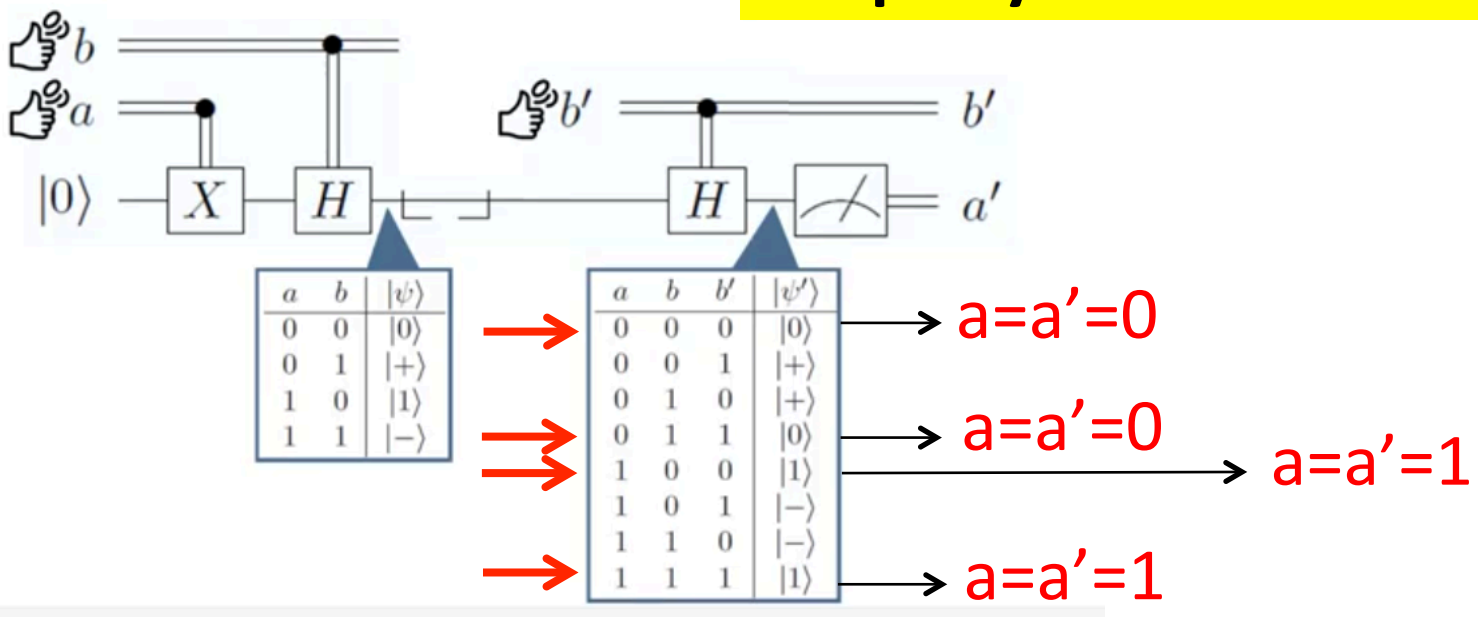
BB84 protocol

Now, Bob measures |ψ'> in the computational basis |0>, |1>

- When |ψ'>=|0> then a'=0 and when |ψ'>=|1> then a'=1
- When |ψ'>=|+> (resp. |ψ'>=|->) then a'=0 with prob. ½ and a'=1 with prob. ½.

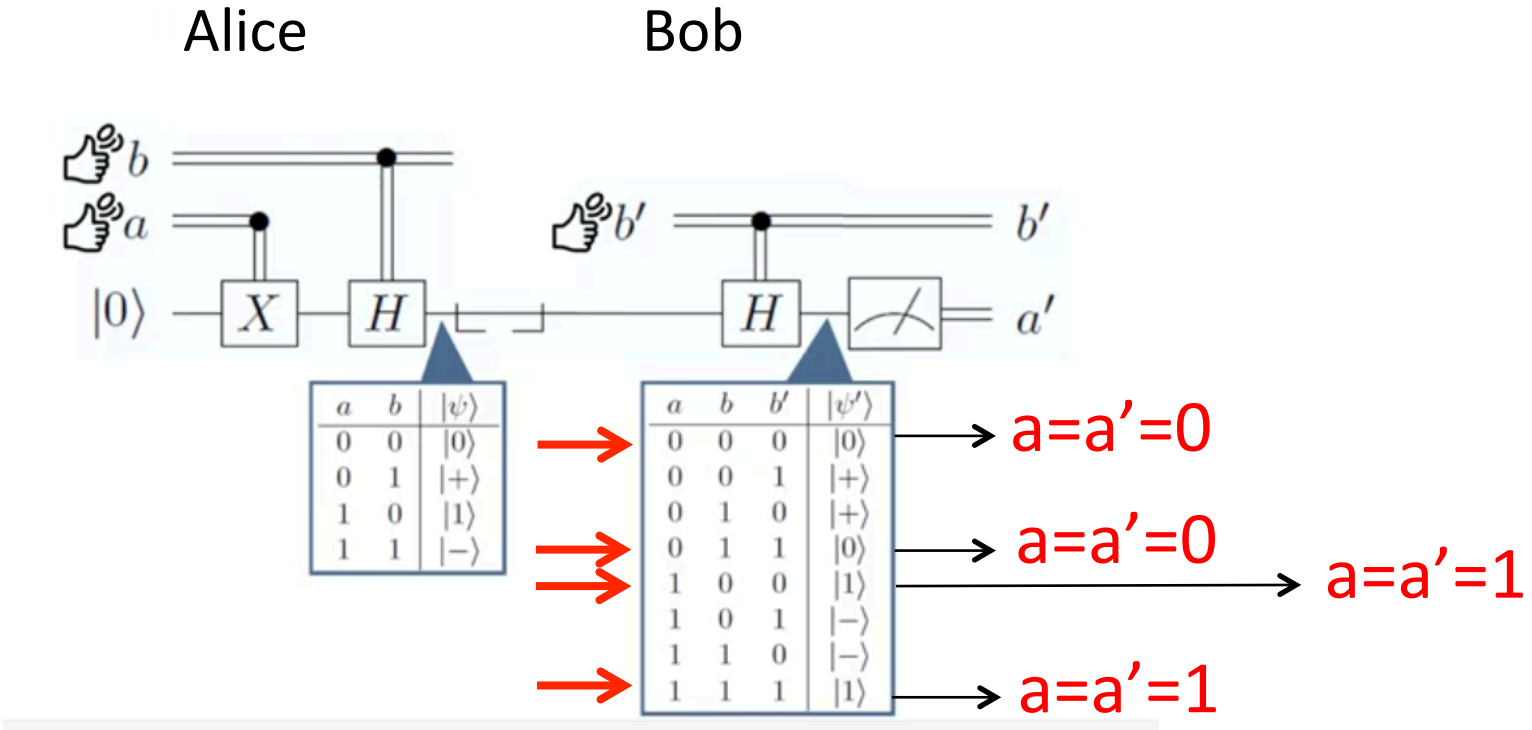
Alice Bob

Property: when b=b' then a=a'



BB84 protocol

- Alice and Bob communicate to each other, possibly publicly, the values of b and b'.
- When b=b', element of secret key is value of a (=a').
- Process is repeated until key long enough.

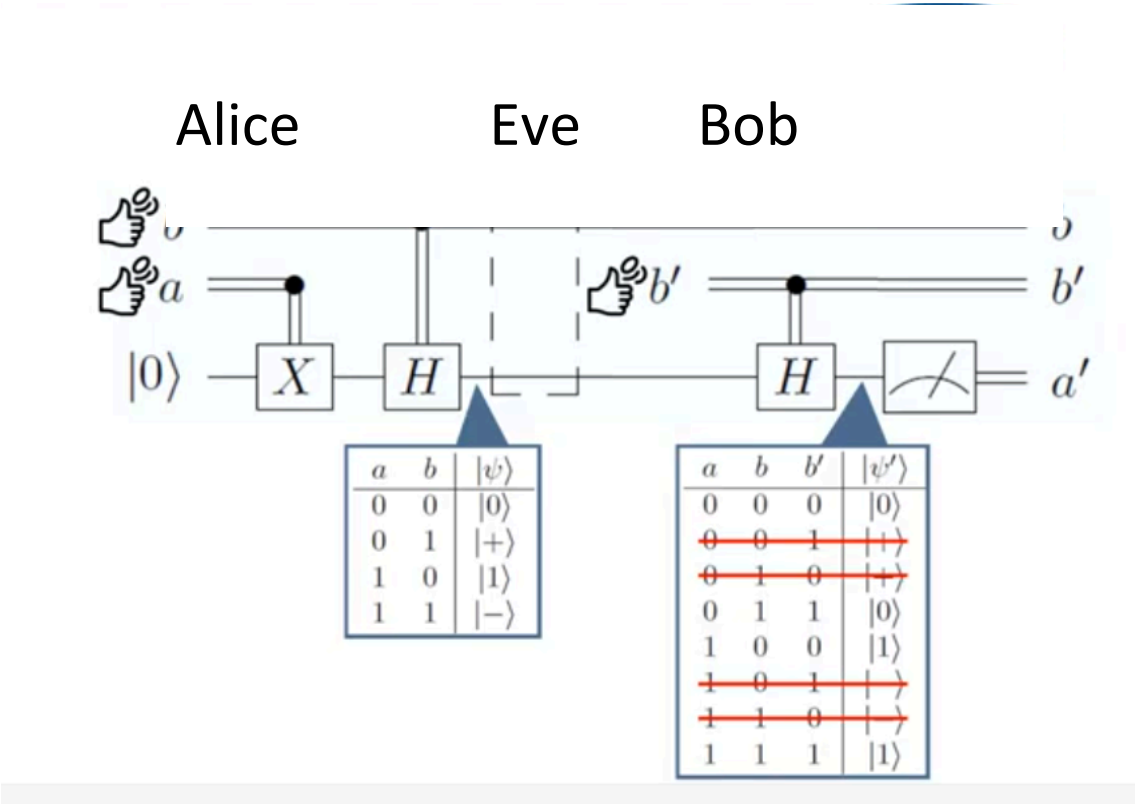


BB84 protocol

Can an eavesdropper (Eve) read Qbit sent by Alice to Bob and find key without being detected?

Answer: No!

BB84 protocol



- Impossible to copy an unkown quantum state
  No cloning theorem
- Eve can only measure and resend Alice's Qbit

BB84 protocol

Case 1: Eve uses computational basis $|0\rangle$ and $|1\rangle$

If $|\psi\rangle = |0\rangle$ then Eve finds $|\psi\rangle = |0\rangle$.
If $|\psi\rangle = |1\rangle$ then Eve finds $|\psi\rangle = |1\rangle$.
In both cases, measurement does not disturb quantum state.

However, if $|\psi\rangle = |+\rangle$ then Eve finds $|\psi\rangle = |0\rangle$ with prob. ½ and $|\psi\rangle = |1\rangle$ with prob. ½.
Similarly, if $|\psi\rangle = |-\rangle$ then Eve finds $|\psi\rangle = |0\rangle$ with prob. ½ and $|\psi\rangle = |1\rangle$ with prob. ½.
In both cases, measurement disturbs quantum state.

BB84 protocol

Case 1 (cont'): Eve uses computational basis |0> and |1>

Since a and b are random, |ψ> can either be in state |0>, |1|, |+> or |-> with prob. ¼.

Therefore, a fraction of Qbits will always be disturbed by Eve's measurement.

When disturbance it is no longer true that when b=b' then a=a

BB84 protocol

Case 1 (cont'): Eve uses computational basis |0> and |1>

When there is disturbance, it is no longer true that when b=b' then a=a'.

Example: a=0, b=1. Then |ψ>=|+>

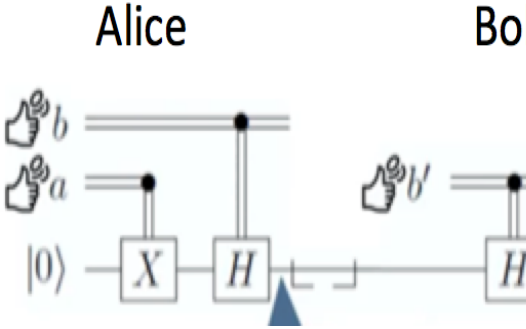
a	b	|ψ'⟩
0	0	|0⟩
0	1	|+⟩
1	0	|1⟩
1	1	|−⟩

Assume after Eve's measurement |ψ>=|0>

(this occurs with prob. ½ ; with prob. ½ |ψ>=|1>).

Assume b'=1. Then H|0>=|+>.

However, a'=1 with prob. ½ and a'=0 with prob. ½ as Bob is measuring in basis |0>, |1>.



➔ It is no longer guarantee that when b=b' then a=a'.

BB84 protocol

Case 2: Eve uses Hadamard basis |+> and |->

Same reasoning yields same conclusion, i.e. there is no guarantee that when b=b’ then a=a’.

BB84 protocol

What can then Alice and Bob do to secure communication?

Answer:

- Create key as described before, namely, Alice uses key $(a_1,\ldots,a_n)$ and uses key $(a'_1,\ldots, a'_n)$, with n typically large (several thousands).
- Pick a sample: they agree on the phone « let's select digits in positic

5, 34, 76, 104, 203 » (of course sample is much larger than that)

- $(a_5,a_{34},a_{76},a_{104},a_{203}) \neq (a'_5,a'_{34},a'_{76},a'_{104},a'_{203})$ communication disturbed (presence of eavesdropper)
- $(a_5,a_{34},a_{76},a_{104},a_{203}) = (a'_5,a'_{34},a'_{76},a'_{104},a'_{203})$ communication secu

Can be shown about ¼ of digits are different if eavesdropper.

Communication protocols that use a few Qbits

- Quantum cryptography
  - BB84 protocol
  - E91 protocol
- Quantum dense coding
- Quantum teleportation

Quantum cryptography: E91 protocol

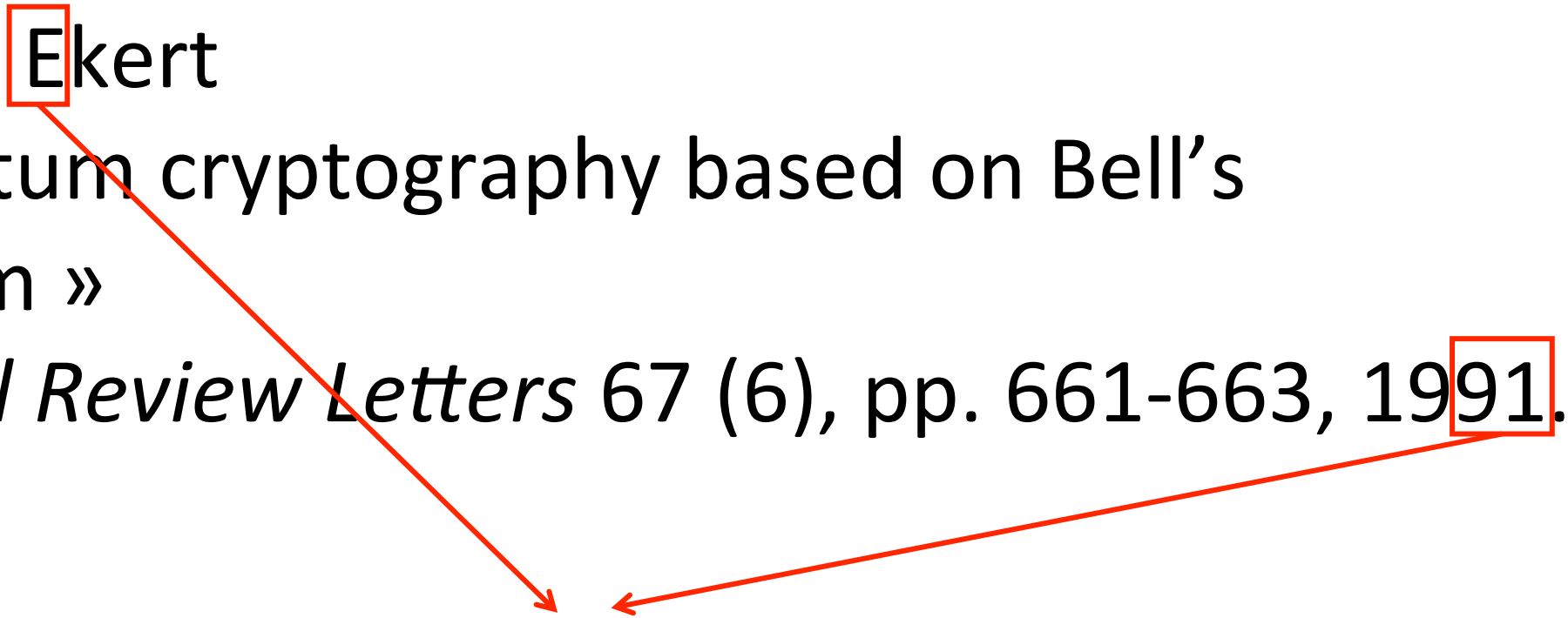
Artur K. Ekert
« Quantum cryptography based on Bell's theorem »
Physical Review Letters 67 (6), pp. 661-663, 1991.

Quantum cryptography: E91 protocol

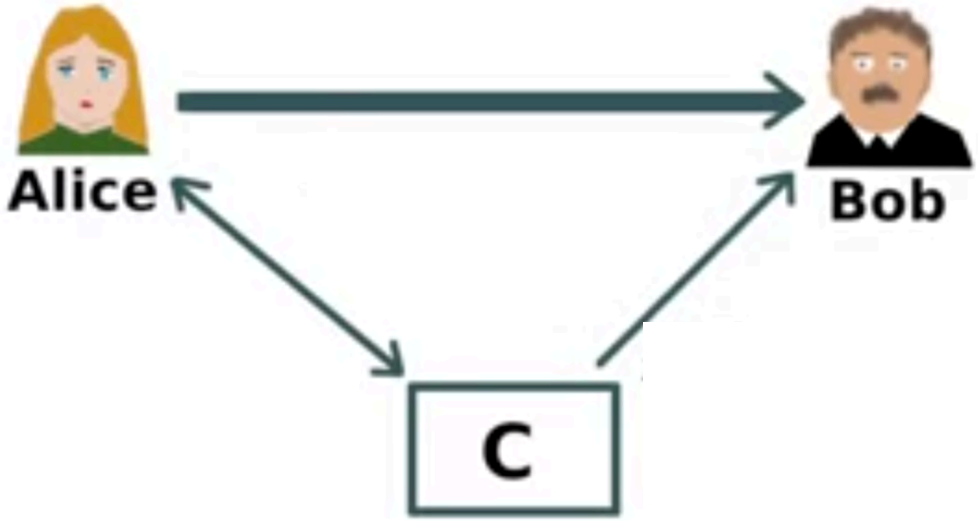
Artur K. Ekert

« Quantum cryptography based on Bell's theorem »

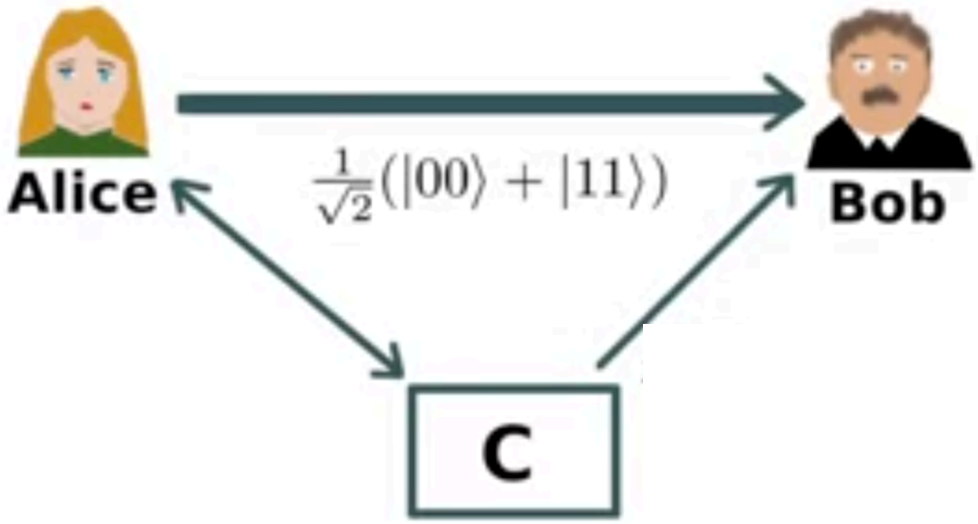
Physical Review Letters 67 (6), pp. 661-663, 1991.



E91 protocol



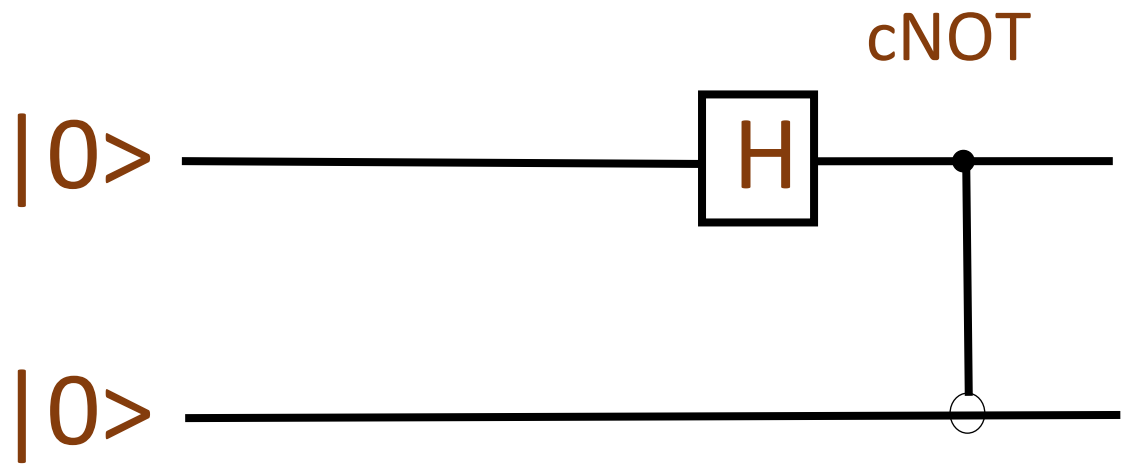
E91 protocol



- Alice asks third party (C) to generate pairs of entangled photons: one photon goes to Alice, other photon goes to Bob

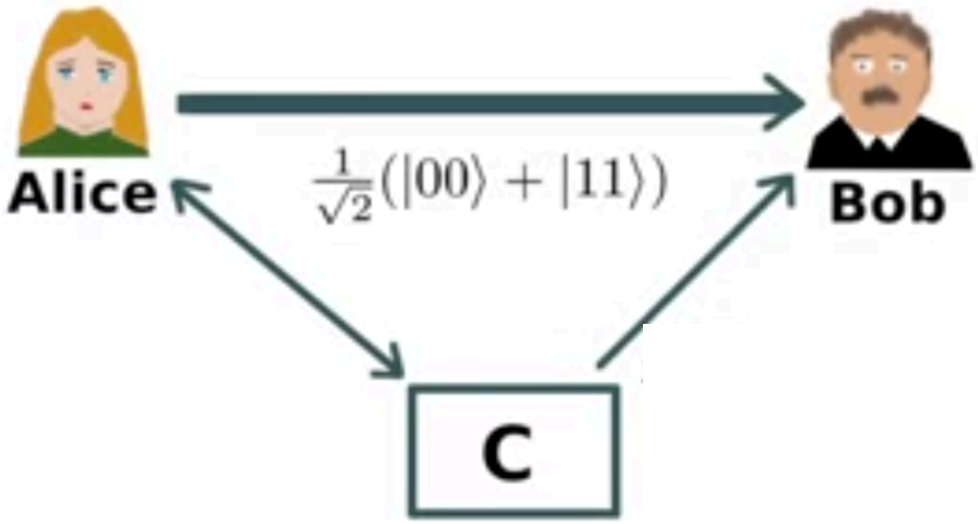
E91 protocol

Reminder: 2-Qbit entangled state (Bell state)



$$|00\rangle \xrightarrow{H} (|00\rangle+|10\rangle)/\sqrt{2} \xrightarrow{cNOT} (|00\rangle+|11\rangle)/\sqrt{2}$$

E91 protocol

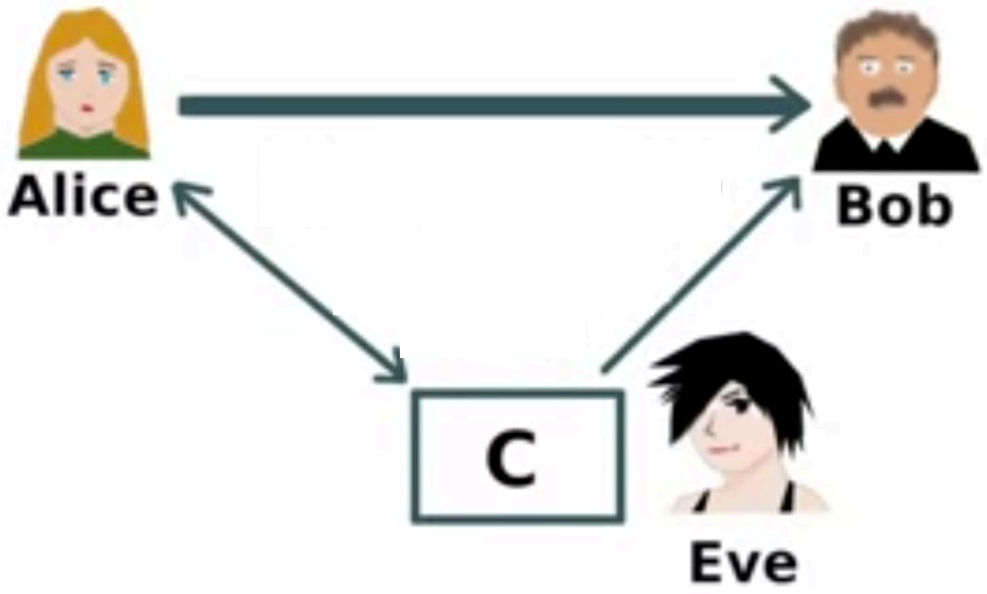


C does not know values measured by Alice and Bob as all outcomes are random

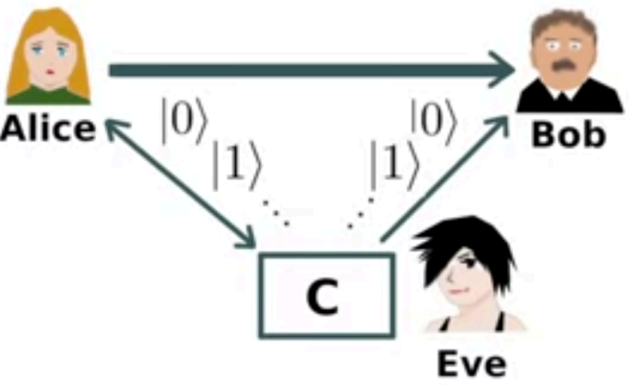
- Alice asks third party (C) to generate pairs of entangled photons: one photon goes to Alice, other photon goes to Bob
- When Alice and Bob measure in the |0>, |1> basis they find same value, 0 with prob. ½ , 1 with prob. ½
- Repeating this operation n times gives shared key with n bits.

E91 protocol

Problem: Eavesdropper (Eve) may intercept entangled photon sent by C to Alice and Bob.



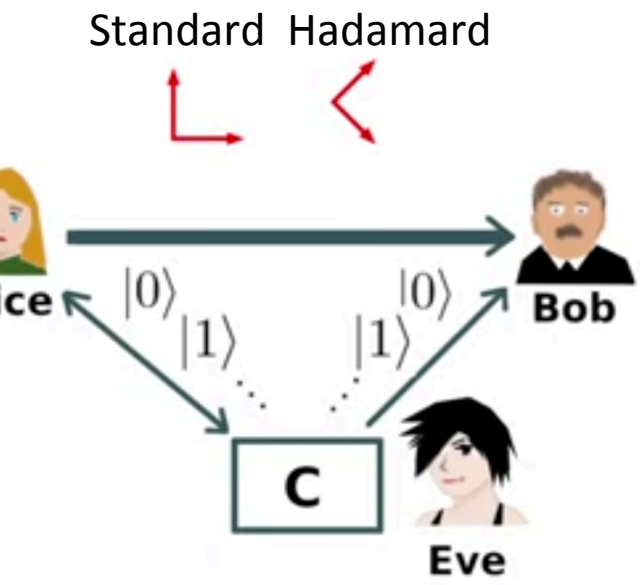
E91 protocol



Eve randomly prepares pairs states |0>,|0> or |1>, and send photons to Alice and Bob.
Alice and Bob still have the same result for each measurement.
But Eve knows these results!

Fix: for each bit of shared key, Alice and Bob choose either standard basis |0>, |1| with prob. ½ or Hadamard (H) basis |+>,|-> with prob. ½.
They always agree to use the same basis (need not be secured).

E91 protocol



❑ When entangled Qbits are sent to Alice and Bob

$$\frac{1}{\sqrt{2}}(|0>|0>+|1>|1>)$$

$$\xrightarrow{HH}\frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}(|0>+|1>).\frac{1}{\sqrt{2}}(|0>+|1>))+\frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}(|0>-|1>).\frac{1}{\sqrt{2}}(|0>-|1>))$$

$$=\frac{1}{2\sqrt{2}}(|0>|0>+|0>|1>+|1>|0>+|1>|1>+|0>|0>-|0>|1>-|1>|0>+|1$$

$$=\frac{1}{2\sqrt{2}}(2|0>|0>+2|1>|1)=\frac{1}{\sqrt{2}}(|0>|0>+|1>|1)$$

Alice and Bob always observe same value! (0 with prob. ½ and 1 with pro

❑ When non-entangled Qbits are sent to Alice and Bob

$$|0>|0>\xrightarrow{HH}\frac{1}{\sqrt{2}}(|0>+|1>).\frac{1}{\sqrt{2}}(|0>+|1>)$$

$$|1>|1>\xrightarrow{HH}\frac{1}{\sqrt{2}}(|0>-|1>).\frac{1}{\sqrt{2}}(|0>-|1>)$$

Alice and Bob may observe different values,
i.e. observe values (1,0) or (0,1) each with prob. ¼

E91 protocol

Once Alice and Bob each have constructed a sequence with n bits, they randomly choose some of them and check whether they are equal (similar to BB84).

The more bits they check the more confident they are about absence of eavesdropper.

If some bits are different they stop transmission and report to

Existing implementations of QKD

BB84 protocol is used today for most quantum key distributions (QKD) implementations.

In 2007, NIST (National Institute of Standards and Technology) announced realization on optical fiber of 148.7 km15.

BB84 protocol is supported on several networks including DARPA QKD16, SECOCQ QKD17, Tokyo QKD18.

Existing implementations QKD

A network for quantum key distribution (QKD) spanning thousands of kilometres has been built in China.

System comprises 2000 km fibre optic link between Shanghai, Hefei, Jinan and Beijing and a satellite link spanning 2600 km between two observatories – one east of Beijing and the other just a few hundred kilometres from China's border with Kazakhstan.

Communication protocols that use a few Qbits

- Quantum cryptography
  - BB84 protocol
  - E91 protocol
- Quantum dense coding
- Quantum teleportation

Quantum dense coding

If Alice prepares a Qbit in state $|\psi\rangle$ and sends it to Bob, all he can do is to apply a unitary transformation of his choice and then measure the Qbit, obtaining the value 0 or 1.

After that the Qbit is either in the state $|0\rangle$ or $|1\rangle$ and no further measurement can teach him anything about its initial state $|\psi\rangle$.

- The most Alice can communicate to Bob by sending him a single Qbit is a single bit of information.

Quantum dense coding

Assume that Alice has one member of an entangled pair of Qbits in the state

$$|\psi\rangle=(|0\rangle_a|0\rangle_b+|1\rangle_a|1\rangle_b)/\sqrt{2}$$

and Bob has the other one.

Quantum dense coding

By suitable preparing her member of the pair and then sending it to Bob, Alice can convey to him two bits of Information.

How?

Quantum dense coding

Alice may want to convey the two bits 00, 01, 10, or 11.
To this end, she first applies the transformation **I**, **X**, **Z**, or **ZX** to her Qbit, depending on whether she wants to send Bob the message 00, 01, 10, or 11. This gives

Alice sends to Bob

00 $\Rightarrow$ $I_a|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_a|0\rangle_b + |1\rangle_a|1\rangle_b)$

01 $\Rightarrow$ $X_a|\psi\rangle = \frac{1}{\sqrt{2}}(|1\rangle_a|0\rangle_b + |0\rangle_a|1\rangle_b)$

10 $\Rightarrow$ $Z_a|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_a|0\rangle_b - |1\rangle_a|1\rangle_b)$

11 $\Rightarrow$ $Z_aX_a|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_b - |1\rangle_a|0\rangle_b)$

Quantum dense coding

$$>= \frac{1}{\sqrt{2}}(|0>_a|0>_b + |1>_a|1>_b)$$

$$>= \frac{1}{\sqrt{2}}(|1>_a|0>_b + |0>_a|1>_b)$$

$$>= \frac{1}{\sqrt{2}}(|0>_a|0>_b - |1>_a|1>_b)$$

$$|\psi>= \frac{1}{\sqrt{2}}(|0>_a|1>_b - |1>_a|0>_b)$$

Alice sends her Qbit over to Bob.

Bob sends the pair through the controlled-NOT gate C using the Qbit he received from Alice as control and hi Qbit as target.

eminder: the C-NOT gate operates on a quantum register consisting of two Qbits. It flips the 2nd Qbit (the target Qbit) iff the 1st Qbit (the control Qbit) is |1>.

Before		After	
ontrol	Target	Control	Target
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

$$C_{a,b}I_a|\psi>= \frac{1}{\sqrt{2}}(|0>_a|0>_b + |1>_a|0>_b) = \frac{1}{\sqrt{2}}(|0>_a + |1>_a)|0>_b$$

$$C_{a,b}X_a|\psi>= \frac{1}{\sqrt{2}}(|1>_a|1>_b + |0>_a|1>_b) = \frac{1}{\sqrt{2}}(|0>_a + |1>_a)|1>_b$$

$$C_{a,b}Z_a|\psi>= \frac{1}{\sqrt{2}}(|0>_a|0>_b - |1>_a|0>_b) = \frac{1}{\sqrt{2}}(|0>_a - |1>_a)|0>_b$$

$$C_{a,b}Z_aX_a|\psi>= \frac{1}{\sqrt{2}}(|0>_a|1>_b - |1>_a|1>_b) = \frac{1}{\sqrt{2}}(|0>_a - |1>_a)|1>_b$$

... Bob applies CNOT to the received state

Quantum dense coding

$$I_a|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_a + |1\rangle_a)|0\rangle_b$$

$$X_a|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_a + |1\rangle_a)|1\rangle_b$$

$$Z_a|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_a - |1\rangle_a)|0\rangle_b$$

$$Z_a X_a|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_a - |1\rangle_a)|1\rangle_b$$

Bob then applies a Hadamard transformation to Alice's Qbit

$$H_a C_{a,b} I_a|\psi\rangle = |0\rangle_a|0\rangle_b \Rightarrow 00$$

$$H_a C_{a,b} X_a|\psi\rangle = |0\rangle_a|1\rangle_b \Rightarrow 01$$

$$H_a C_{a,b} Z_a|\psi\rangle = |1\rangle_a|0\rangle_b \Rightarrow 10$$

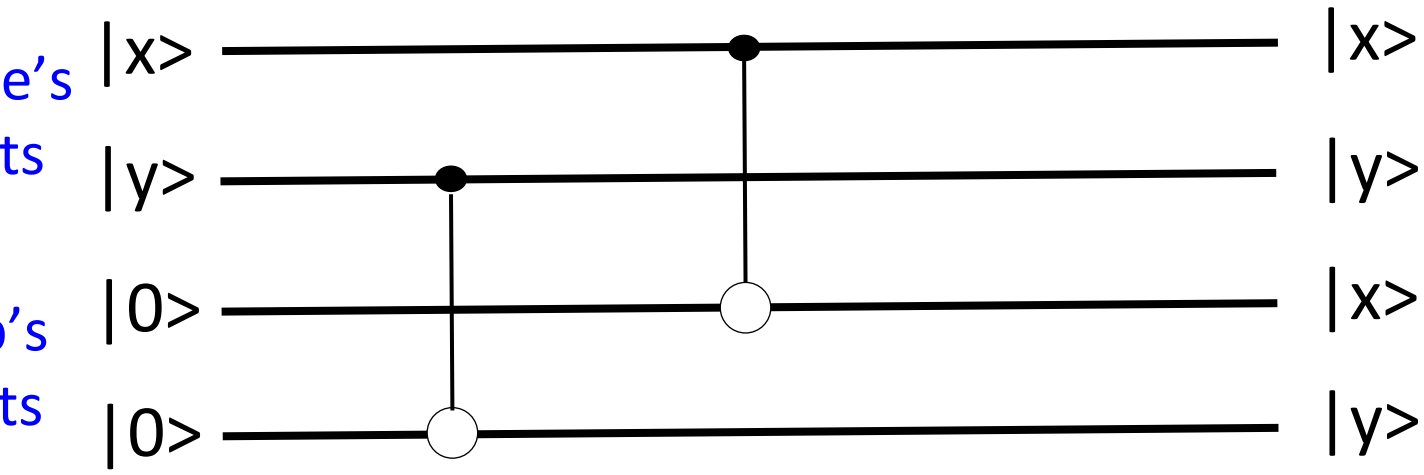
$$H_a C_{a,b} Z_a X_a|\psi\rangle = |1\rangle_a|1\rangle_b \Rightarrow 11$$

BOB APPLIES HADAMARD TO GET THE MESSAGE

Measuring the Qbits gives Bob 00, 01, 10, or 11 – precisely the two-bit message Alice wished to send!

Quantum dense coding

A circuit-theoretic representation of quantum dense coding



with x,y=0,1. If x = 1 (resp. y=1) then Bob's first (resp. second) Qbit is flipped, otherwise Bob's first (resp. second) Qbit is unchanged.

Communication protocols that use a few Qbits

- Quantum cryptography
  - BB84 protocol
  - E91 protocol
- Quantum dense coding
- Quantum teleportation

Quantum teleportation

C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres,
nd W. K. Wootters,
« Teleporting an unknown quantum state via dual classical
nd Einstein-Podolsky-Rosen Channels »
Physical Review Letters, vol. *70,* pp. 1895-1899, 1993.

Quantum teleportation

Suppose Alice has a Qbit in state

$$|\psi\rangle = \alpha|0\rangle_{a_1} + \beta|1\rangle_{a_1}$$

$$|\alpha|^2 + |\beta|^2 = 1$$

Alice <u>does not know</u> the amplitudes α and β.

Reminder: when a measurement is made, with prob. $|\alpha|^2$ the Qbit is found in state 0 and with prob. $|\beta|^2$ the Qbit is found in state 1.

Quantum teleportation

In addition to Qbit $|\psi>$, Alice has another Qbit that she shares with Bob (more next).

One wants to find a way so that Bob's Qbit state inherits Alice's Qbit state. More precisely, state assignement acquired by Bob's Qbit will no longer apply to Alice's ➡ **transported from her Qbit to hi**

Alice is allowed to send « classical information » to Bob (can ta to him over phone, send e-mail,…).

Quantum teleportation

Trivial way: Alice sends Qbit to Bob.

But what if Alice does not want (e.g. for technical reasons) to do that?

Quantum teleportation

Alice's second Qbit and Bob's Qbit share the 2-Qbit entangled state (Bell state)

$$|\Phi>=\frac{1}{\sqrt{2}}(|0>_{a_2}|0>_b+|1>_{a_2}|1>_b)$$

with subscripts a_2 (resp. b) referring to Alice's Qbits (resp. Bob's).

Quantum teleportation

Alice's second Qbit and Bob's Qbit share the 2-Qbit entangled state (Bell state)

$$|\Phi>=\frac{1}{\sqrt{2}}(|0>_{a_2}|0>_b+|1>_{a_2}|1>_b)$$

This means that upon measurement, with prob. ½ both Qbits will found in state 0 and with prob. ½ both Qbits will be found in stat

Notice that storing two entangled particles for more than a brief time is not easy (it had not been achieved when Bennett et. al pa appeared in 1993) but has now been achieved by several teams worldwide.

Quantum teleportation

Here is how teleportation works.
Alice's first Qbit and entangled pair she shares with Bob are characterized by 3-Qbit state

$$|\psi>|\Phi>=(\alpha|0>_{a_1}+\beta|1>_{a_1})\frac{1}{\sqrt{2}}(|0>_{a_2}|0>_b+|1>_{a_2}|1>_b)$$

$$=\alpha|0>_{a_1}\frac{1}{\sqrt{2}}(|0>_{a_2}|0>_b+|1>_{a_2}|1>_b)+\beta|1>_{a_1}\frac{1}{\sqrt{2}}(|0>_{a_2}|0>_b+|1>_{a_2}|1>_b$$

Quantum teleportation

3-Qbit state: $\alpha|0\rangle_{a_1}\frac{1}{\sqrt{2}}(|0\rangle_{a_2}|0\rangle_b+|1\rangle_{a_2}|1\rangle_b)+\beta|1\rangle_{a_1}\frac{1}{\sqrt{2}}(|0\rangle_{a_2}|0\rangle_b+|1\rangle_{a_2}|1\rangle_b)$

To teleport the unknown state of her Qbits to Bob's member of the entangled pair, Alice first applies a cNOT gate, using her 1st Qbit in state $|\psi\rangle$ as control and her member of shared entangled pair as target. This produces the 3-Qbit state

$$\alpha|0\rangle_{a_1}\frac{1}{\sqrt{2}}(|0\rangle_{a_2}|0\rangle_b+|1\rangle_{a_2}|1\rangle_b)+\beta|1\rangle_{a_1}\frac{1}{\sqrt{2}}(|1\rangle_{a_2}|0\rangle_b+|0\rangle_{a_2}|1\rangle_b)$$

Quantum teleportation

3-Qbit state: $\alpha|0>_{a_1} \frac{1}{\sqrt{2}}(|0>_{a_2}|0>_b + |1>_{a_2}|1>_b) + \beta|1>_{a_1} \frac{1}{\sqrt{2}}(|1>_{a_2}|0>_b + |0>_{a_2}|1>$

Next, she applies a Hadamard transformation **H** to her 1st Qbit

($H|0>_{a_1} = \frac{1}{\sqrt{2}}(|0>_{a_1} + |1>_{a_1})$, $H|1>_{a_1} = \frac{1}{\sqrt{2}}(|0>_{a_1} - |1>_{a_1})$), yielding

$$\alpha\frac{1}{\sqrt{2}}(|0>_{a_1} + |1>_{a_1})\frac{1}{\sqrt{2}}(|0>_{a_2}|0>_b + |1>_{a_2}|1>_b) + \beta\frac{1}{\sqrt{2}}(|0>_{a_1} - |1>_{a_1})\frac{1}{\sqrt{2}}(|1>_{a_2}|0>_b + |0>_{a_2}|1>_b)$$

$$= \frac{1}{2}|0>_{a_1}|0>_{a_2}(\alpha|0>_b + \beta|1>_b) + \frac{1}{2}|1>_{a_1}|0>_{a_2}(\alpha|0>_b - \beta|1>_b)$$

$$+ \frac{1}{2}|0>_{a_1}|1>_{a_2}(\alpha|1>_b + \beta|0>_b) + \frac{1}{2}|1>_{a_1}|1>_{a_2}(\alpha|1>_b - \beta|0>_b)$$

* WHAT A CAN MEASURE

* (SOEIN OO VA BŌ NŌ)

Quantum teleportation

Now, Alice measures both Qbits in her possession.

If result is 00, Bob's Qbit will indeed acquire state $|\psi>$ originally possessed by Alice's 1st Qbit, (whose state will then be reduced to |0>).

Quantum teleportation

f result is 10, 01, or 11 then Bob's Qbit becomes

$$\alpha|0\rangle_b - \beta|1\rangle_b, \quad \alpha|1\rangle_b + \beta|0\rangle_b, \quad \text{or} \quad \alpha|1\rangle_b - \beta|0\rangle_b$$

n each of these three cases, there exists a unitary transformation that restores state of Bob's Qbit to Alice's original state $|\psi\rangle$

- 1st case apply **Z** (leaves |0>, changes sign of |1>)
- 2nd case apply **X** (interchange |0> and |1>)
- 3rd case apply **ZX**

Quantum teleportation

o, all Alice needs to do to transfer the state of
er Qbit to Bob's member of the entangled pair,
to **telephone** Bob and **report to him the state of**
f her two measurements.

ob then knows if the state has already been transfer
f Alice's result is 00) or what unitary transformation
, **X**, or **ZX**) he must apply to his member of the
ntangled pair to complete the transfer (teleportatio

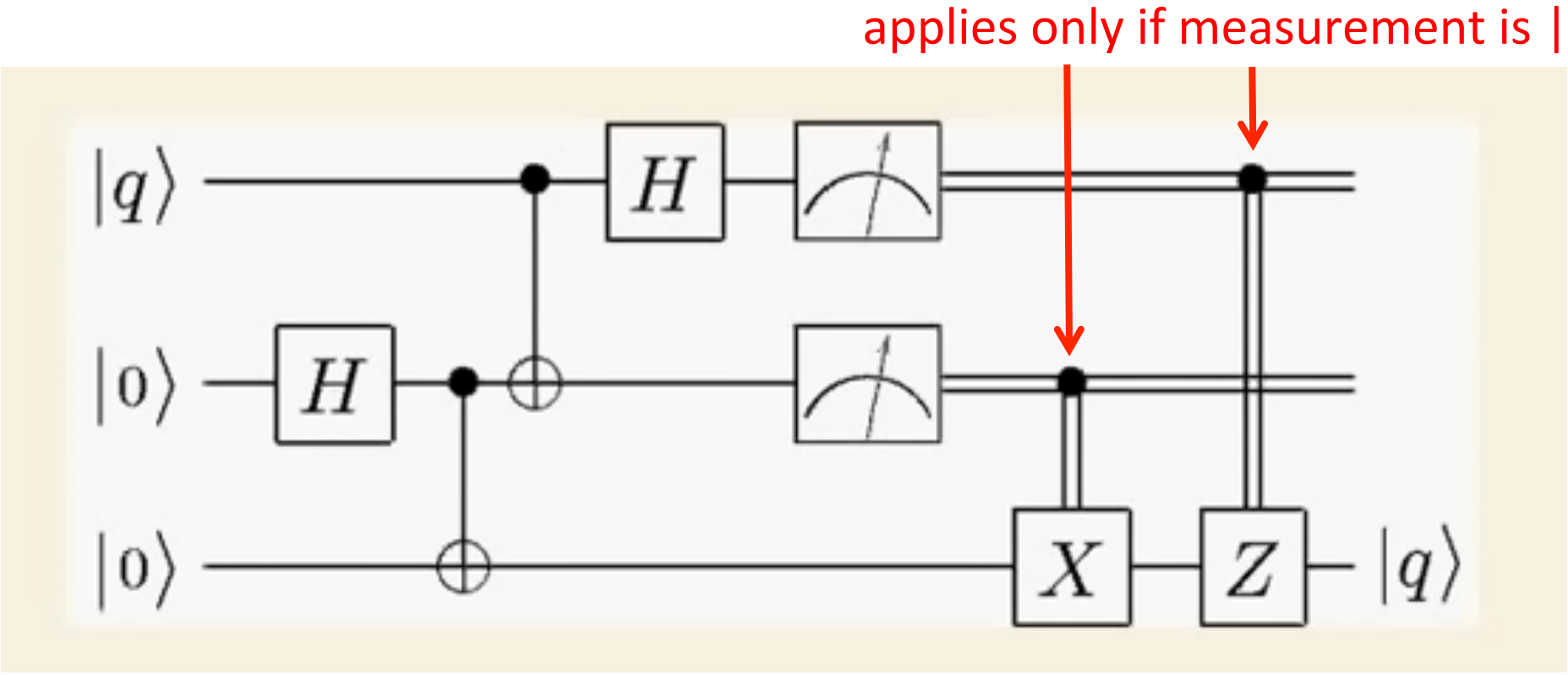
Quantum teleportation

his appears to be remarkable! A general state of a bit is described by two complex numbers α and β that ke on a continuum of values, only constrained by the quirement that $|\alpha|^2 + |\beta|^2 = 1.$

et, with aid of standard entangled pair, whose state oes not depend on α and β, Alice is able to provide Bob ith a Qbit described by the unknown state, at the price of **nly two classical bits of information** and the **loss of ntanglement of their pair.**

Quantum teleportation

rcuit-theoretic representation of teleportation protocol



it’s time to come back to earth

UNIVE
CÔTE D

No-cloning theorem

There is no unitary transformation that can take the state $|\Psi\rangle|0\rangle$ into the state $|\Psi\rangle|\Psi\rangle$ for arbitrary $|\Psi\rangle$.

Proof. If $\mathbf{U}(|\Psi\rangle|0\rangle) = |\Psi\rangle|\Psi\rangle$ and $\mathbf{U}(|\varphi\rangle|0\rangle) = |\varphi\rangle|\varphi\rangle$ it follows by linearity

$$\mathbf{U}(a|\Psi\rangle + b|\varphi\rangle)|0\rangle = a\mathbf{U}|\Psi\rangle|0\rangle + b\mathbf{U}|\varphi\rangle|0\rangle$$
$$= a|\Psi\rangle|\Psi\rangle + b|\varphi\rangle|\varphi\rangle. \qquad (1)$$

But if **U** cloned arbitrary inputs, we would have

$$\mathbf{U}(a|\Psi\rangle + b|\varphi\rangle)|0\rangle = (a|\Psi\rangle + b|\varphi\rangle)\,(a|\Psi\rangle + b|\varphi\rangle)$$
$$= a^2|\Psi\rangle|\Psi\rangle + b^2|\varphi\rangle|\varphi\rangle + ab|\Psi\rangle|\varphi\rangle + ab|\varphi\rangle|\Psi\rangle$$

which differs from (1) unless $a = 1, b = 0$ or $a = 0, b = 1$ or $a = b = 0$.

https://www.youtube.com/watch?v=8NiLxXQDNps

https://www.youtube.com/watch?v=g_IaVepNDT4

https://www.youtube.com/watch?v=hRFQd_fkzws

How to visually represent a Qbit when amplitudes α and β are complex numbers?

Since α = Re(α) + i.Im(α) and β= Re(β) + i.Im(β) a 4D space is needed
Not too convenient for a graphic representation …

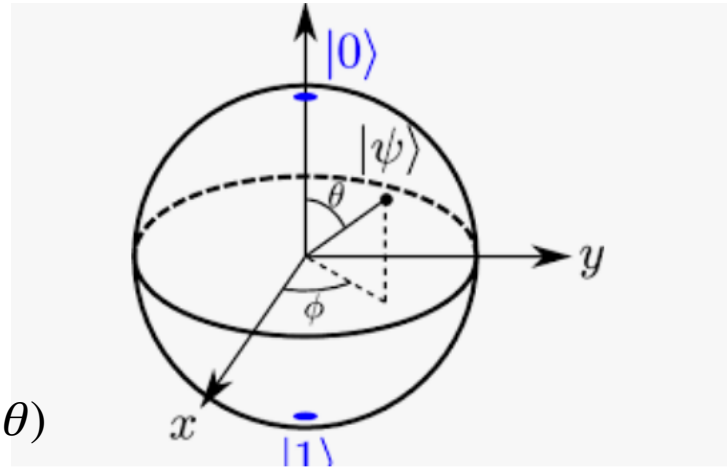
Solution: on a unit sphere (called Bloch sphere)

In this representation

$$|0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \text{ and } |1\rangle = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}$$

θ, φ give the unique point (x,y,z)

with $x=\sin(\theta)\cos(\varphi), y = \sin(\theta)\sin(\varphi), z = \cos(\theta)$



Quick reminder (see lectures 1 & 2)

- State of a pair of Qbits = their tensor product

If $|\psi>_i = \alpha_i |0> + \beta_i |1>$, $|\alpha_i|^2 + |\beta_i|^2 = 1$, $i=1,2$, state of $(|\psi>_1, |\psi>_2)$ is

$$|\psi>_1 \otimes |\psi>_2 =$$

$$(\alpha_1 |0> + \beta_1 |1>) \otimes (\alpha_2 |0> + \beta_2 |1>) = \left(\alpha_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) \otimes \left(\alpha_2 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$$

$$= \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{pmatrix} \quad \text{with} \quad \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} \quad \text{vector tensor product.}$$

Note that $\text{entry}_1 \,.\, \text{entry}_4 = \text{entry}_2 \,.\, \text{entry}_3 = \alpha_1\alpha_2\,\beta_1\beta_2$

Quick reminder (see lectures 1 & 2)

- Superposition of two Qbits (**2-Qbit**) = any normalized superposition of four orthogonal classical states.

$$\alpha_{00}|00>+\alpha_{01}|01>+\alpha_{10}|10>+\alpha_{11}|11>=\alpha_{00}\begin{pmatrix}1\\0\\0\\0\end{pmatrix}+\alpha_{01}\begin{pmatrix}0\\1\\0\\0\end{pmatrix}+\alpha_{10}\begin{pmatrix}0\\0\\1\\0\end{pmatrix}+\alpha_{11}\begin{pmatrix}0\\0\\0\\1\end{pmatrix}=\begin{pmatrix}\alpha_{00}\\\alpha_{01}\\\alpha_{10}\\\alpha_{11}\end{pmatrix},$$

with $|\alpha_{00}|^2+|\alpha_{01}|^2+|\alpha_{10}|^2+|\alpha_{11}|^2=1$. Here $|ab>=|a>\otimes|b>$. E.g. $|10>=|1>\otimes|0>=\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\0\\1\\0\end{pmatrix}$.

A general 2-Qbit state is a special form of the state of pair of Qbits iff $\alpha_{00}\alpha_{11}=\alpha_{01}\alpha_{10}$.

Such nonproduct states of two or more Qbits are called entangled states.