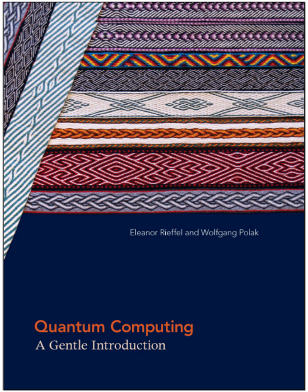
# PHYS 407 - Introduction to Quantum Computing

Term: Spring 2023
Meetings: Tuesday & Thursday 10:00-11:15
Location: Room 201 Stuart Building
Video: All sessions recorded for online viewing

Instructor: Carlo Segre
Office: 166D/172 Pritzker Science
Phone: 312.567.3498
email: segre@iit.edu




Resources: *Quantum Computing: A Gentle Introduction*, E. Rieffel & W. Polak (MIT Univ Press, 2011)

*Introduction to Classical and Quantum Computing*, T. Wong (Rooted Grove, 2022)

*Quirk: A drag-and-drop quantum circuit simulator*, Craig Gidney

Web Site: http://phys.iit.edu/∼segre/phys407/23S

# Course objectives

1. Clearly describe the building blocks of quantum computing.
2. Apply tools of quantum computing to manipulate qubits.
3. Clearly describe the fundamental hardware used to realize quantum computers.
4. Clearly describe the purpose and realization of quantum gates.
5. Use the concept of quantum entanglement to develop quantum algorithms.
6. Clearly describe the techniques of quantum error correction and fault tolerance.
7. Build quantum algorithms using Quirk.

# Course grading

30% – Homework assignments
Weekly, due at beginning of class
Turned in via Blackboard

40% – Exams

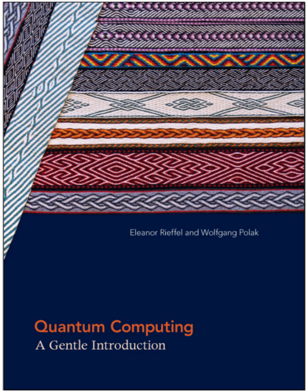
30% – Final project/presentation?

Grading scale

| | | | | |
|---|---|---|---|---|
| A | – | 88% | to | 100% |
| B | – | 75% | to | 88% |
| C | – | 62% | to | 75% |
| D | – | 50% | to | 62% |
| E | – | 0% | to | 50% |

# Topics to be covered (chapter titles)

1. Quantum building blocks
2. Quantum algorithms
3. Entagled subsystems and robust computation
4. Quantum computing hardware
5. Other topics as appropriate



# Why study quantum computing?

Quantum computing is one part of a broader field called quantum information science which has revolutionized cryptography and secure communications

Quantum computing can provide solutions to problems that are computationally expensive using digital computers

Quantum computing error correction and fault tolerance has made the technology practical

Companies are beginning to build practical quantum computers with many qubits

Quantum computing is becoming interesting to a number of fields outside physics and could be even more relevant in the near future

# Today's outline - January 10, 2023

- Quantum fundamentals
- Superposition
- Dirac notation
- Qubits & linear algebra
- Quantum postulates
- Quantum key distribution

Reading Assignment: Reiffel: 2.4-2.5; 3.1 Wong: 2.2.2-2.4.3; 4.2.1-4.2.2

Homework Assignment #01:
due Thursday, January 19, 2023

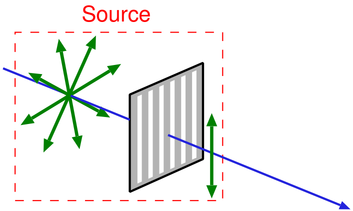
# Quantum mechanics fundamentals

A quantum computer is built of qubits which consist of physical systems which have two measureable states

A simple example of such a system is the polarization of a photon

Consider an unpolarized beam of light from a laser pointer prepared in the vertical polarization by a filter

A detector for the vertical state will detect the full beam intensity, A detector for the horizontal state will detect nothing



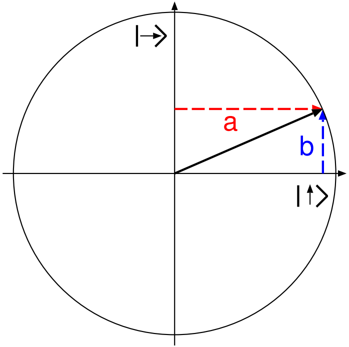

If a tilted polarizer is placed in between, the horizontal detector now measures a smaller, but non-zero, value

Because photons are quantum particles, this effect works even for single photons with the measuring a fraction of the photons to be horizontal

# Superposition of states

The state of a single photon can be represented generalized quantum superposition of the $|\uparrow\rangle$ and $|\rightarrow\rangle$ states

The amplitudes $a$ and $b$ are complex constants such that the state is normalized




$$|v\rangle = a|\uparrow\rangle + b|\rightarrow\rangle,$$

$$|v|^2 \equiv 1 \quad \longrightarrow \quad |a|^2 + |b|^2 = 1$$

$$a = |a|e^{i\alpha}, \quad b = |b|e^{i\beta}$$

Suppose a photon in a general state $|v\rangle$ enters a detector whose direction is $|\uparrow\rangle$

The probability of detection is $|a|^2$ and the probability of absorption is $|b|^2$

This formalism allows us to describe the polarization experiment

# Polarizer experiment

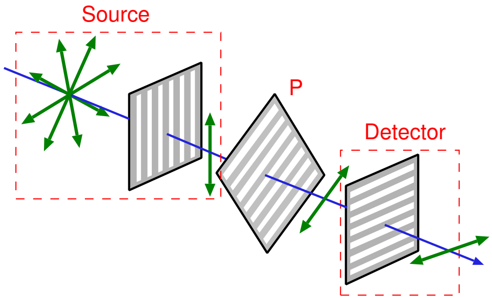
The photons that come from the source are in a state $|\uparrow\rangle$

In the axes of the polarizer $P$ there are two possible states $|\nearrow\rangle$ and $|\nwarrow\rangle$ and the vertically polarized photon can be written as

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}|\nearrow\rangle + \frac{1}{\sqrt{2}}|\nwarrow\rangle$$

The photon thus has an 0.5 probability of passing through the polarizer and will then be in a state

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle$$




Again there is only an 0.5 probability of the photon passing so an initial photon will have a probability of $0.5 \times 0.5 = 0.25$ of making it to the detector

Quantum particles (and qubits) behave probabilistically

# Dirac notation

Any two-state quantum system can be considered a qubit and can be modeled as a superposition of the two linearly independent states

$$|q\rangle = a|0\rangle + b|1\rangle, \qquad a = |a|e^{i\alpha}, \qquad b = |b|e^{i\beta}$$

Examples include photon polarization, electron spin, and ground/excited states of atoms

The infinte number of possible states in this system can all be described by the linear superposition $|q\rangle$

Dirac, or bra-ket, notation is used to describe quantum systems. The ket ($|x\rangle$) and bra ($\langle x|$) are used to represent a vector and its conjugate transpose respectively

A complex vector space $V$ is generated by a set of vectors, $S$, if every $|v\rangle \in V$ can be written as a complex linear superposition of the vectors in the set

$$|v\rangle = a_1|s_1\rangle + a_2|s_2\rangle + \cdots + a_n|s_n\rangle, \quad |s_i\rangle \in S, \quad a_i = |a_i|e^{i\varphi_i}$$

# Dirac notation (cont.)

The span of $S$ is the subspace of all linear combinations of vectors in $S$

A basis, $B$, is a set of vectors for which every element of $V$ can be written as a unique linear combination of vectors $|b\rangle \in B$

In a two-dimensional space such as a qubit, any two vectors which are not multiples of each other and are orthonormal form a basis

For polarized photons, $\{|\uparrow\rangle, |\rightarrow\rangle\}$, $\{|\nearrow\rangle, |\nwarrow\rangle\}$, and $\{|\circlearrowright\rangle, |\circlearrowleft\rangle\}$ are all valid basis sets

Operations on the vector space $V$ include the inner (scalar, dot) product $\langle v_2|v_1\rangle$ with properties

$$\langle v|v\rangle = Re\{\langle v|v\rangle\} > 0$$

$$\langle v_2|v_1\rangle = \overline{\langle v_1|v_2\rangle}$$

$$(a\langle v_2| + b\langle v_3|)|v_1\rangle = a\langle v_2|v_1\rangle + b\langle v_3|v_1\rangle$$

A basis set $B = \{|\beta_1\rangle, |\beta_2\rangle, \dots |\beta_n\rangle\}$ is said to be orthonormal if

$$\langle \beta_i|\beta_j\rangle = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

# Vector representation of a qubit

In order to represent a qubit, it is necessary to select a standard basis set, $\{|0\rangle, |1\rangle\}$, of two orthonormal vectors

The specific physical states used for this standard basis is not important but must remain fixed

In quantum information processing, the $\{|0\rangle, |1\rangle\}$ basis has a direct correspondence to the classical 0 and 1 bits

The major difference is that qubits can take on an infinite number of superpositions of $|0\rangle$ and $|1\rangle$

For a basis $\{|\beta_1\rangle, |\beta_2\rangle\}$, an arbitrary ket $|v\rangle$ can be written as a vector in the language of linear algebra

$$|v\rangle = a|\beta_1\rangle + b|\beta_2\rangle \quad \longrightarrow \quad v = \begin{pmatrix} a \\ b \end{pmatrix}$$

# Similarity to linear algebra

The ket, $|\alpha\rangle$, corresponds to a column vector, $\alpha$, in linear algebra while a bra $\langle\alpha|$ is its conjugate transpose, $\alpha^\dagger$, a row vector

$$|\alpha\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \quad \langle\alpha| = (\overline{a_1} \; \cdots \; \overline{a_n})$$

The inner product of two vectors is

$$\langle\alpha|\beta\rangle = (\overline{a_1} \; \cdots \; \overline{a_n}) \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \sum_{i=1}^{n} \overline{a_i} b_i$$

Gates are just operators that act on vectors as linear transformations.

$$G|\alpha\rangle = \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & & \vdots \\ g_{n1} & \cdots & g_{nn} \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

In the standard basis, $\{|0\rangle, |1\rangle\}$, the vector $|v\rangle = a|0\rangle + b|1\rangle$ is

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad |v\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$$

# Postulates of quantum mechanics

Quantum computing requires an understanding of the postulates of quantum mechanics, specifically how measurements are performed

Given a 2-state system, quantum mechanics states that there can only be two results from a measurement, the eigenvalues of the system in the basis that is being used for measurement

The probability of obtaining a specific result is determined by the square of the magnitude of the amplitude of that result in the superposition state of the system

consider the measurement of a photon by a vertical polarization detector, the basis is

$$\{|\uparrow\rangle, |\rightarrow\rangle\}$$

The state of the photon can be expressed as

$$|\gamma\rangle = a|\uparrow\rangle + b|\rightarrow\rangle$$

A measurement by the vertical polarization detector will give

Photon present with probability $|a|^2$

No photon present with probability $|b|^2$

After the measurement any photon that passed through the polarizer is now in the $|\uparrow\rangle$ state

# More quantum principles

A quantum state may be a superposition in the standard basis but not in another basis

$$|\alpha\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = |+\rangle, \qquad \{|+\rangle, |-\rangle\} \equiv \left\{ \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \right\}$$

A superposition is not just a probabilistic mixture of two states, it is a definite state which consists of both its constitutent states

Qubits can exist in an infinite number of superposition states yet do not contain more information than classical bits since a single measurement produces only one of two answers depending on the basis

There is much more to quantum theory but this is sufficient to develop a theory of quantum computing

Realizing an actual quantum computer requires a deep knowledge of quantum mechanics and experimental quantum systems

# Quantum cryptography

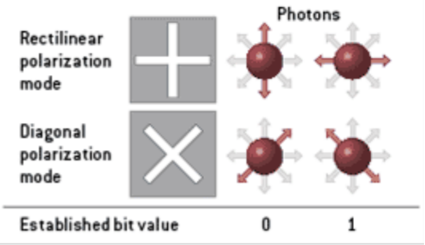
Quantum cryptography is not about sending entire messages using quantum systems

Instead messages are sent using standard cryptography means with secret keys

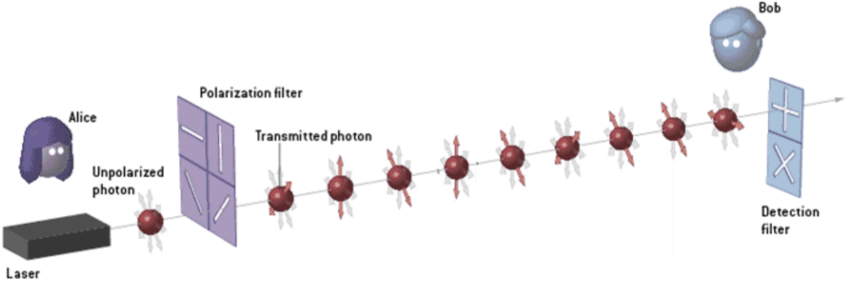
Computer-generated secret keys, even if long, are theoretically subject to cracking with enough computing power

The solution is to exchange the secret key using the combination of a quantum channel and a public channel

Use photons polarized in two of three possible basis sets (rectilinear, diagonal, circular) and assign 0 and 1 bit values to each polarization direction possible



# Quantum cryptography implementation



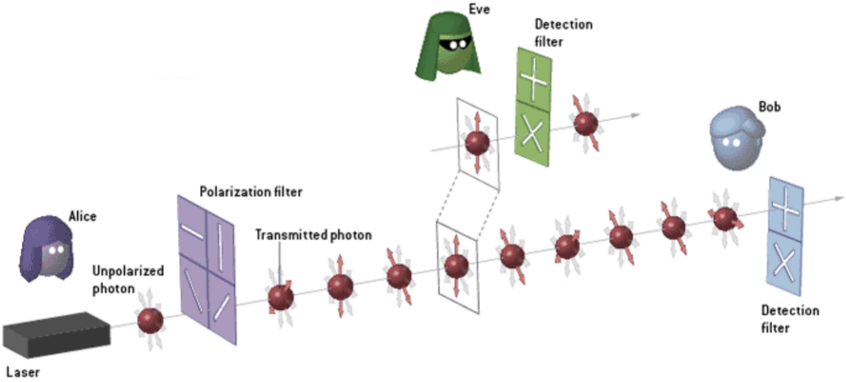

1. Alice chooses and records the filter type and the bit value for a series of photons sent
2. Bob measures each incoming photon with a random choice of filter and records the choice and result
3. Bob tells Alice his filter choices on a public channel and Alice confirms which of his filters were correct
4. The remaining bits form the key that Bob and Alice can use

http://blogs.scientificamerican.com/guest-blog/2012/11/20/quantum-cryptography-at-the-end-of-your-road/

# Key distribution procedure

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Alice's random bit | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
| Alice's random basis | $+$ | $+$ | $\times$ | $+$ | $\times$ | $\times$ | $\times$ | $+$ |
| Polarization sent | $\uparrow$ | $\rightarrow$ | $\searrow$ | $\uparrow$ | $\searrow$ | $\nearrow$ | $\nearrow$ | $\rightarrow$ |
| Bob's random basis | $+$ | $\times$ | $\times$ | $\times$ | $+$ | $\times$ | $+$ | $+$ |
| Polarization measured | $\uparrow$ | $\nearrow$ | $\searrow$ | $\nearrow$ | $\rightarrow$ | $\nearrow$ | $\rightarrow$ | $\rightarrow$ |
| Public discussion | Y | | Y | | | Y | | Y |
| Shared secret key | 0 | | 1 | | | 0 | | 1 |

# Eavesdropping scheme




Suppose that Eve attempts to intercept a photon by measuring with a particular basis and then passing the resulting photon on to Bob

An error may be created if Eve chooses the wrong filter

# Key distribution with eavesdropper

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Alice's random bit | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
| Alice's random basis | $+$ | $+$ | $\times$ | $+$ | $\times$ | $\times$ | $\times$ | $+$ |
| Polarization sent | $\uparrow$ | $\rightarrow$ | $\searrow$ | $\uparrow$ | $\searrow$ | $\nearrow$ | $\nearrow$ | $\rightarrow$ |
| Eve's random basis | $+$ | $\times$ | $+$ | $+$ | $\times$ | $+$ | $\times$ | $+$ |
| Eve's polarization | $\uparrow$ | $\nearrow$ | $\rightarrow$ | $\uparrow$ | $\searrow$ | $\rightarrow$ | $\nearrow$ | $\rightarrow$ |
| Bob's random basis | $+$ | $\times$ | $\times$ | $\times$ | $+$ | $\times$ | $+$ | $+$ |
| Polarization measured | $\uparrow$ | $\nearrow$ | $\nearrow$ | $\searrow$ | $\rightarrow$ | $\nearrow$ | $\uparrow$ | $\rightarrow$ |
| Public discussion | Y | | Y | | | Y | | Y |
| Shared secret key | 0 | | 0 | | | 0 | | 1 |

# Detecting eavesdroppers

Eve can be detected with high probability by comparing a sufficiently large number of transmitted bits, resulting in some added waste

Eve's probability of choosing the incorrect basis is 50%

When Bob measures an intercepted photon with the correct basis, he has 50% chance of getting the incorrect result

Probability of having an error with the correct basis is 25%

By comparing $n$ key bits, the probability of detecting Eve is $P_d = 1 - \left(\frac{3}{4}\right)^n$

To detect Eve with $P_d = 1 \times 10^{-9}$ requires $n = 72$

# Experimental quantum cryptography


PHYSICAL REVIEW LETTERS

VOLUME 70 | 29 MARCH 1993 | NUMBER 13


## Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels


Charles H. Bennett,[1] Gilles Brassard,[2] Claude Crépeau,[2,3] Richard Jozsa,[2] Asher Peres,[4] and William K. Wootters[5]

[1] *IBM Research Division, T.J. Watson Research Center, Yorktown Heights, New York 10598*

[2] *Département IRO, Université de Montréal, C.P. 6128, Succursale "A", Montréal, Québec, Canada H3C 3J7*

[3] *Laboratoire d'Informatique de l'École Normale Supérieure, 45 rue d'Ulm, 75230 Paris CEDEX 05, France*[a]

[4] *Department of Physics, Technion—Israel Institute of Technology, 32000 Haifa, Israel*

[5] *Department of Physics, Williams College, Williamstown, Massachusetts 01267*



(Received 2 December 1992)



An unknown quantum state $|\phi\rangle$ can be disassembled into, then later reconstructed from, purely classical information and purely nonclassical Einstein-Podolsky-Rosen (EPR) correlations. To do so the sender, "Alice," and the receiver, "Bob," must prearrange the sharing of an EPR-correlated pair of particles. Alice makes a joint measurement on her EPR particle and the unknown quantum system, and sends Bob the classical result of this measurement. Knowing this, Bob can convert the state of his EPR particle into an exact replica of the unknown state $|\phi\rangle$ which Alice destroyed.



PACS numbers: 03.65.Bz, 42.50.Dv, 89.70.+c


The existence of long range correlations between Einstein-Podolsky-Rosen (EPR) [1] pairs of particles raises the question of their use for information transfer. Einstein himself used the word "telepathically" in this context [2]. It is known that *instantaneous* information transfer is definitely impossible [3]. Here, we show that EPR correlations can nevertheless assist in the "teleportation" of an intact quantum state from one place to another, by a sender who knows neither the state to be teleported nor the location of the intended receiver.

Suppose one observer, whom we shall call "Alice," has been given a quantum system such as a photon or spin-$\frac{1}{2}$ particle, prepared in a state $|\phi\rangle$ unknown to her, and she wishes to communicate to another observer, "Bob," sufficient information about the quantum system for him to make an accurate copy of it. Knowing the state vector $|\phi\rangle$ itself would be sufficient information, but in general there is no way to learn it. Only if Alice knows beforehand that $|\phi\rangle$ belongs to a given orthonormal set can she make a measurement whose result will allow her to make an accurate copy of $|\phi\rangle$. Conversely, if the possibilities for $|\phi\rangle$ include two or more nonorthogonal states, then no measurement will yield sufficient information to prepare a perfectly accurate copy.

A trivial way for Alice to provide Bob with all the information in $|\phi\rangle$ would be to send the particle itself. If she wants to avoid transferring the original particle, she can make it interact unitarily with another system, or "ancilla," initially in a known state $|a_0\rangle$, in such a way that after the interaction the original particle is left in a standard state $|\phi_0\rangle$ and the ancilla is in an unknown state $|a\rangle$ containing complete information about $|\phi\rangle$. If Alice now sends Bob the ancilla (perhaps technically easier than sending the original particle), Bob can reverse her actions to prepare a replica of her original state $|\phi\rangle$. This "spin-exchange measurement" [4] illustrates an essential feature of quantum information: it can be swapped from one system to another, but it cannot be duplicated or "cloned" [5]. In this regard it is quite unlike classical information, which can be duplicated at will. The most tangible manifestation of the nonclassicality of quantum information is the violation of Bell's inequalities [6] observed [7] in experiments on EPR states. Other manifestations include the possibility of quantum cryptography [8], quantum parallel computation [9], and the superiority of interactive measurements for extracting information from a pair of identically prepared particles [10].







The spin-exchange method of sending full information to Bob still lumps classical and nonclassical information together in a single transmission. Below, we show how Alice can divide the full information encoded in $|\phi\rangle$ into two parts, one purely classical and the other purely nonclassical, and send them to Bob through two different channels. Having received these two transmissions, Bob can construct an accurate replica of $|\phi\rangle$. Of course Alice's original $|\phi\rangle$ is destroyed in the process, as it must be to obey the no-cloning theorem. We call the process we are about to describe teleportation, a term from science fiction meaning to make a person or object disappear while an exact replica appears somewhere else. It must be emphasized that our teleportation, unlike some science fiction versions, defies no physical laws. In particular, it cannot take place instantaneously or over a spacelike interval, because it requires, among other things, sending a classical message from Alice to Bob. The net result of teleportation is completely prosaic: the removal of $|\phi\rangle$ from Alice's hands and its appearance in Bob's hands a suitable time later. The only remarkable feature is that, in the interim, the information in $|\phi\rangle$ has been cleanly separated into classical and nonclassical parts. First we shall show how to teleport the quantum state $|\phi\rangle$ of a spin-$\frac{1}{2}$ particle. Later we discuss teleportation of more complicated states.

The nonclassical part is transmitted first. To do so, two spin-$\frac{1}{2}$ particles are prepared in an EPR singlet state

$$|\Psi_{23}^{(-)}\rangle = \sqrt{\tfrac{1}{2}}\,(|\uparrow_2\rangle|\downarrow_3\rangle - |\downarrow_2\rangle|\uparrow_3\rangle). \tag{1}$$

The subscripts 2 and 3 label the particles in this EPR pair. Alice's original particle, whose unknown state $|\phi\rangle$ she seeks to teleport to Bob, will be designated by a subscript 1 when necessary. These three particles may be of different kinds, e.g., one or more may be photons, the polarization degree of freedom having the same algebra as a spin.

One EPR particle (particle 2) is given to Alice, while the other (particle 3) is given to Bob. Although this establishes the possibility of nonclassical correlations between Alice and Bob, the EPR pair at this stage contains no information about $|\phi\rangle$. Indeed the entire system, comprising Alice's unknown particle 1 and the EPR pair, is in a pure product state, $|\phi_1\rangle\,|\Psi_{23}^{(-)}\rangle$, involving neither classical correlation nor quantum entanglement between the unknown particle and the EPR pair. Therefore no measurement on either member of the EPR pair, or both together, can yield any information about $|\phi\rangle$. An entanglement between these two subsystems is brought about in the next step.

To couple the first particle with the EPR pair, Alice performs a complete measurement of the von Neumann type on the joint system consisting of particle 1 and particle 2 (her EPR particle). This measurement is performed in the Bell operator basis [11] consisting of $|\Psi_{12}^{(-)}\rangle$ and

$$\begin{aligned}|\Psi_{12}^{(+)}\rangle &= \sqrt{\tfrac{1}{2}}\,(|\uparrow_1\rangle|\downarrow_2\rangle + |\downarrow_1\rangle|\uparrow_2\rangle),\\ |\Phi_{12}^{(\pm)}\rangle &= \sqrt{\tfrac{1}{2}}\,(|\uparrow_1\rangle|\uparrow_2\rangle \pm |\downarrow_1\rangle|\downarrow_2\rangle).\end{aligned} \tag{2}$$

Note that these four states are a complete orthonormal basis for particles 1 and 2.

It is convenient to write the unknown state of the first particle as

$$|\phi_1\rangle = a\,|\uparrow_1\rangle + b\,|\downarrow_1\rangle, \tag{3}$$

with $|a|^2 + |b|^2 = 1$. The complete state of the three particles before Alice's measurement is thus

$$\begin{aligned}|\Psi_{123}\rangle = {}&\frac{a}{\sqrt{2}}\,(|\uparrow_1\rangle|\uparrow_2\rangle|\downarrow_3\rangle - |\uparrow_1\rangle|\downarrow_2\rangle|\uparrow_3\rangle)\\ &+\frac{b}{\sqrt{2}}\,(|\downarrow_1\rangle|\uparrow_2\rangle|\downarrow_3\rangle - |\downarrow_1\rangle|\downarrow_2\rangle|\uparrow_3\rangle).\end{aligned} \tag{4}$$

In this equation, each direct product $|\ _1\rangle|\ _2\rangle$ can be expressed in terms of the Bell operator basis vectors $|\Phi_{12}^{(\pm)}\rangle$ and $|\Psi_{12}^{(\pm)}\rangle$, and we obtain

$$|\Psi_{123}\rangle = \tfrac{1}{2}\,[|\Psi_{12}^{(-)}\rangle\,(-a|\uparrow_3\rangle - b|\downarrow_3\rangle) + |\Psi_{12}^{(+)}\rangle\,(-a|\uparrow_3\rangle + b|\downarrow_3\rangle) + |\Phi_{12}^{(-)}\rangle\,(a|\downarrow_3\rangle + b|\uparrow_3\rangle) + |\Phi_{12}^{(+)}\rangle\,(a|\downarrow_3\rangle - b|\uparrow_3\rangle)]. \tag{5}$$

It follows that, regardless of the unknown state $|\phi_1\rangle$, the four measurement outcomes are equally likely, each occurring with probability 1/4. Furthermore, after Alice's measurement, Bob's particle 3 will have been projected into one of the four pure states superposed in Eq. (5), according to the measurement outcome. These are, respectively,

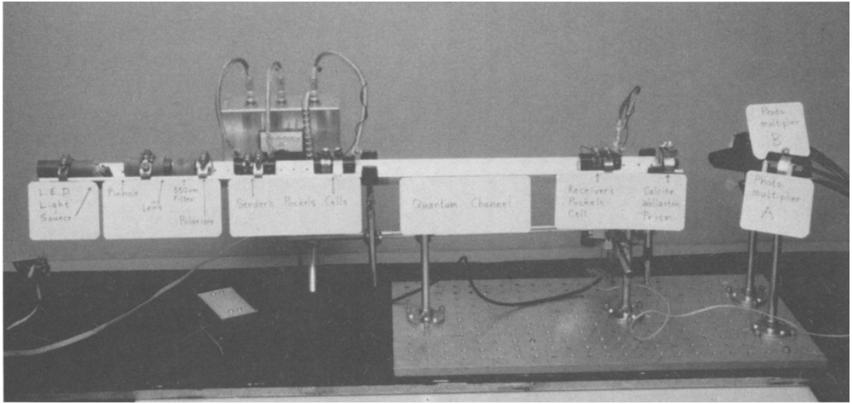
$$\begin{aligned}&-|\phi_3\rangle \equiv -\begin{pmatrix} a\\ b\end{pmatrix}, \quad \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}|\phi_3\rangle,\\ &\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}|\phi_3\rangle, \quad \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}|\phi_3\rangle.\end{aligned} \tag{6}$$

Each of these possible resultant states for Bob's EPR particle is related in a simple way to the original state $|\phi\rangle$ which Alice sought to teleport. In the case of the first (singlet) outcome, Bob's state is the same except for an irrelevant phase factor, so Bob need do nothing further to produce a replica of Alice's spin. In the three other cases, Bob must apply one of the unitary operators in Eq. (6), corresponding, respectively, to 180° rotations around the $z$, $x$, and $y$ axes, in order to convert his EPR particle into a replica of Alice's original state $|\phi\rangle$. (If $|\phi\rangle$ represents a photon polarization state, a suitable combination of half-



"Experimental quantum cryptography," C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *J. Crypt.* **5**, 3-28 (1992).

# First experimental implementation (BB84 protocol)




715,000 pulses $\rightarrow$ 2000 basis matches $\rightarrow$ 754 bit of shared key with eavesdropper having $< 10^{-6}$ bits of information

"Experimental quantum cryptography," C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *J. Crypt.* **5**, 3-28 (1992).