

Quantum key distribution

Paul Dumais
McGill University
January 2002

Information	
Classical	Quantum
may be copied	cannot be copied
may be broadcasted	cannot be broadcasted
may be read and re-read	may be read only once, re-reading causes a collapse

Information (cont'd)	
Classical	Quantum
the unit is the <i>bit</i> which may take two possible values, 0 or 1	a <i>qubit</i> takes a continuum of possible values quantum computation may involve <i>parallelism</i> and <i>interference</i> two quantum states may be <i>entangled</i>

Quantum information: achievements

- Secret key generation by two parties through a public channel (Bennett & Brassard, 1984)
- Element lookup in an unsorted list of size N in expected time $O(\sqrt{N})$ (Grover, 1996)
- Efficient factorization of large integers (Shor, 1997)
- ...

Some qubits

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

$$\alpha, \beta \in \mathbb{C}$$

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

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Some qubits (cont'd)

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

$$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix}$$

$$\frac{\sqrt{2}}{\sqrt{3}}|0\rangle - \frac{i}{\sqrt{3}}|1\rangle = \frac{1}{\sqrt{3}} \begin{bmatrix} \sqrt{2} \\ -i \end{bmatrix}$$

...

Implementation of a qubit

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- Photon polarization

$|0\rangle$: horizontal polarization

$|1\rangle$: vertical polarization

- Electrodynamical cavity

$|0\rangle$: particle not present

$|1\rangle$: particle present

Implementation of a qubit (cont'd)

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- RMN (Magnetic resonance)

$|0\rangle$: up spin

$|1\rangle$: down spin

- Superconductor

$|0\rangle$: current running in one way

$|1\rangle$: current running in the other way

- ...

Unitary operators

$$U^\dagger U = \mathbb{1}$$

$$\mathbb{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} : \begin{cases} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto |1\rangle \end{cases}$$

$$\text{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} : \begin{cases} |0\rangle \mapsto |1\rangle \\ |1\rangle \mapsto |0\rangle \end{cases}$$

$$\sqrt{\text{NOT}} = \begin{bmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{bmatrix} : \begin{cases} |0\rangle \mapsto \frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle \\ |1\rangle \mapsto \frac{1-i}{2}|0\rangle + \frac{1+i}{2}|1\rangle \end{cases}$$

...

The Walsh-Hadamard Operator

$$H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} : \begin{cases} |0\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\ |1\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \end{cases}$$

$$H : \begin{cases} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \mapsto |0\rangle \\ \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \mapsto |1\rangle \end{cases}$$

$$H^2 = \mathbb{1}$$

Measurements (1)

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

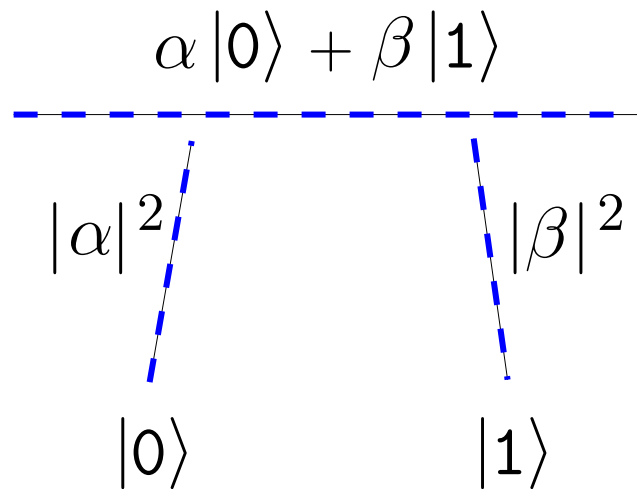
$$\alpha, \beta \in \mathbb{C}$$

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

$$\text{M} : |\Psi\rangle \mapsto \begin{cases} |\alpha|^2 : |0\rangle \\ |\beta|^2 : |1\rangle \end{cases}$$

Measurements (2)

$$\alpha |0\rangle + \beta |1\rangle \text{ --- } \text{---} \left\{ \begin{array}{l} |\alpha|^2 : |0\rangle \\ |\beta|^2 : |1\rangle \end{array} \right.$$



Measurements (3)

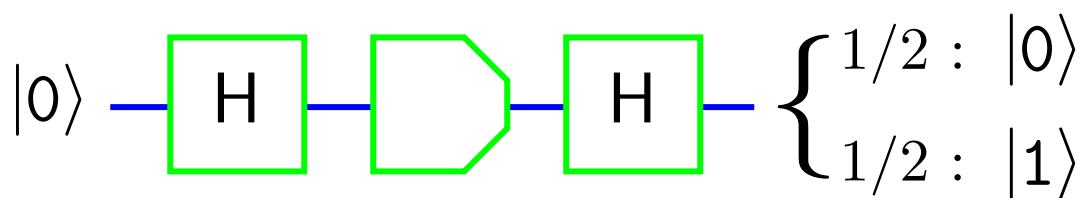
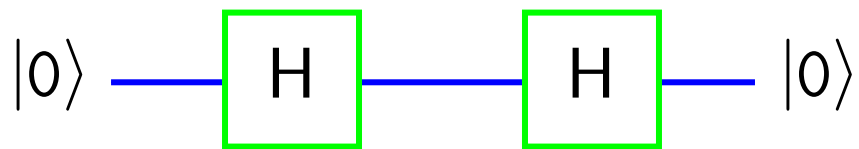
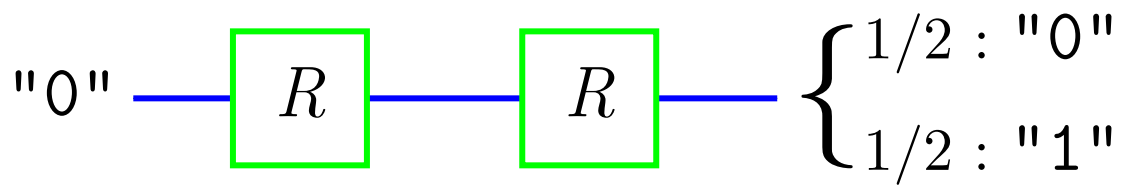
$$\mathbb{M} : |0\rangle \mapsto |0\rangle$$

$$\mathbb{M} : |1\rangle \mapsto |1\rangle$$

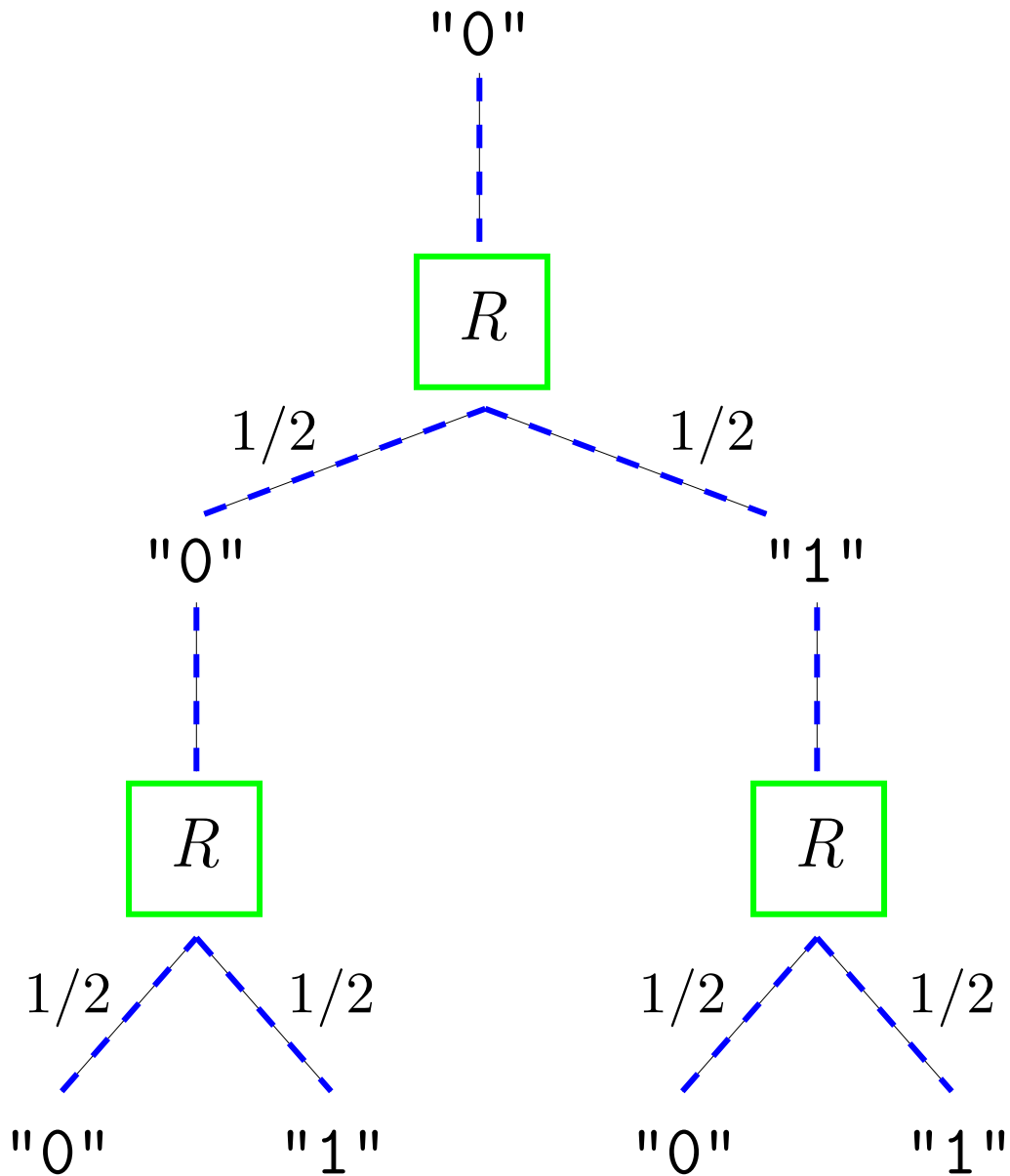
$$\mathbb{M} : \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \mapsto \begin{cases} \frac{1}{2} : |0\rangle \\ \frac{1}{2} : |1\rangle \end{cases}$$

$$\mathbb{M} : \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \mapsto \begin{cases} \frac{1}{2} : |0\rangle \\ \frac{1}{2} : |1\rangle \end{cases}$$

Quantum computation (1)

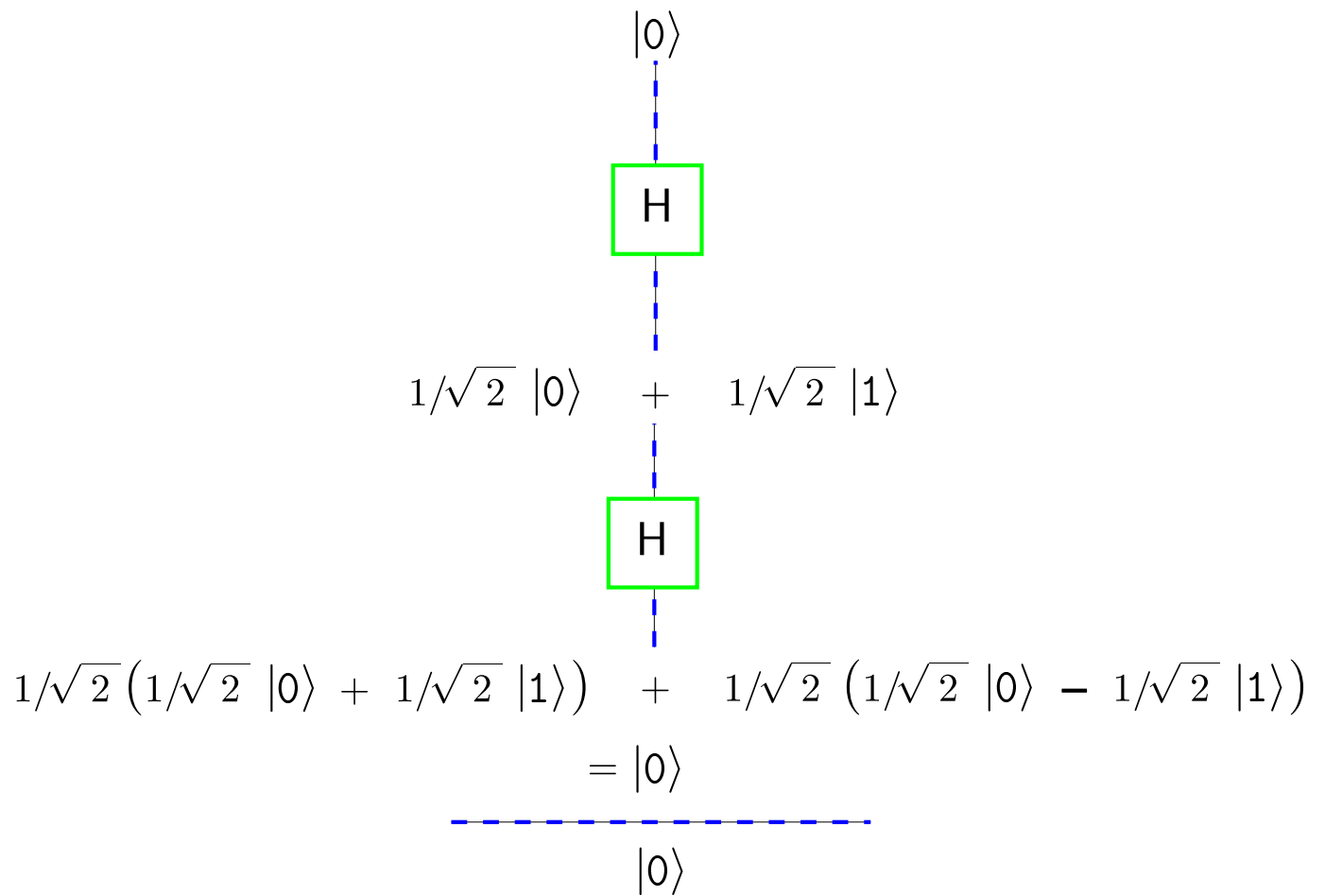


Quantum computation (2)

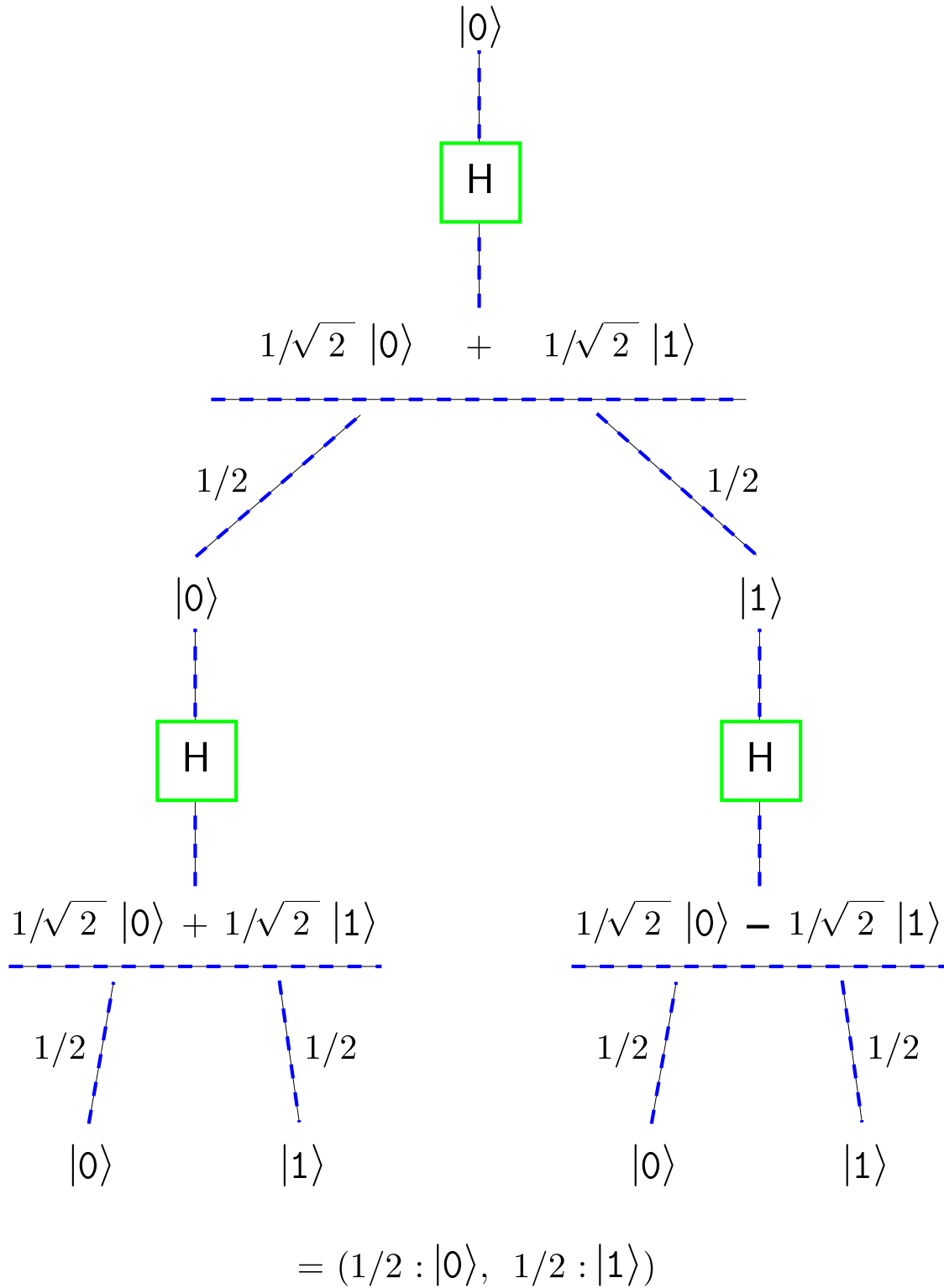


$$= (1/2 : "0", 1/2 : "1")$$

Quantum computation (3)



Quantum computation (4)



Secret key generation

Alice
 $|0\rangle|0\rangle|1\rangle|1\rangle|0\rangle|1\rangle|0\rangle|0\rangle|1\rangle|1\rangle|1\rangle|1\rangle|0\rangle|0\rangle|1\rangle$
H H H H H H H H

Bob
H H H H H H H

 $|0\rangle|0\rangle|1\rangle|1\rangle|0\rangle|0\rangle|1\rangle|0\rangle|1\rangle|0\rangle|1\rangle|1\rangle|0\rangle|1\rangle|1\rangle$
* * * * * * * *

Secret key generation (with adversary)

Alice
 $|0\rangle|0\rangle|1\rangle|1\rangle|0\rangle|1\rangle|0\rangle|0\rangle|1\rangle|1\rangle|1\rangle|1\rangle|0\rangle|0\rangle|1\rangle$
H H H H H H H H

Charles

 $|0\rangle|0\rangle|0\rangle|1\rangle|1\rangle|0\rangle|0\rangle|0\rangle|1\rangle|1\rangle|0\rangle|1\rangle|0\rangle|1\rangle|1\rangle$

Bob

 $|0\rangle|0\rangle|0\rangle|1\rangle|0\rangle|1\rangle|0\rangle|1\rangle|0\rangle|1\rangle|0\rangle|0\rangle|1\rangle|1\rangle|1\rangle|1\rangle$
* * * * * * * * * *
! !