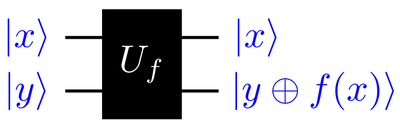
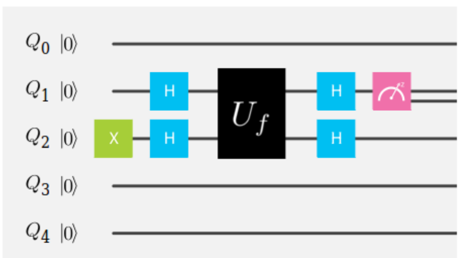
Quantum Computing
Lecture 5

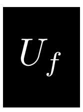
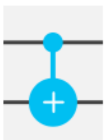
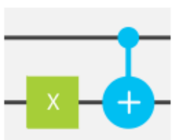
Quantum Information Processing Protocols

Maris Ozols

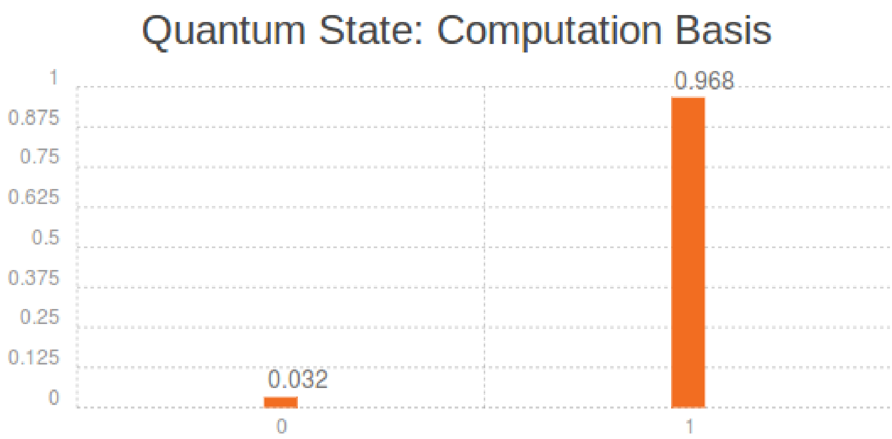
Recap: Deutsch's algorithm



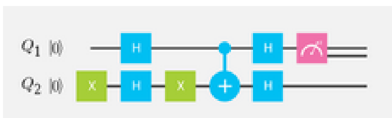


	$f(x) = 0$	$f(x) = x$	$f(x) = 1 \oplus x$	$f(x) = 1$
$f(0)$	0	0	1	1
$f(1)$	0	1	0	1
$f(0) \oplus f(1)$	0	1	1	0
				

And the answer is. . .



Quantum Circuit




```
x q[2];
h q[1];
h q[2];
x q[2];
cx q[1], q[2];
h q[1];
h q[2];
measure q[1];
```

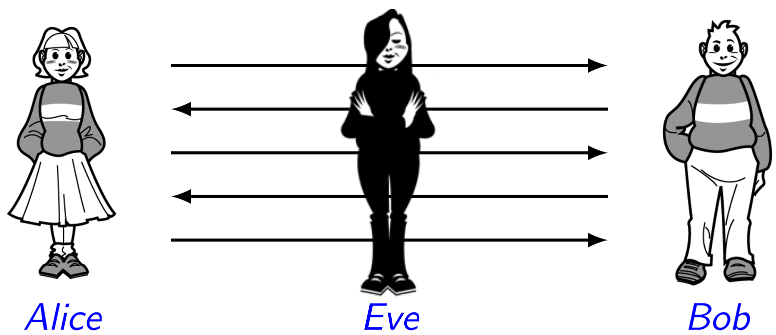
The IBM Quantum Experience:
http://www.research.ibm.com/quantum/

Quantum information: applications

This lecture is on communication and the benefits of using quantum states to encode information. We will discuss three protocols:

- **Quantum key distribution**
- **Superdense coding**
- **Quantum teleportation**

These do not rely on quantum computation as such, but the properties of information encoded in quantum states: superposition and entanglement.



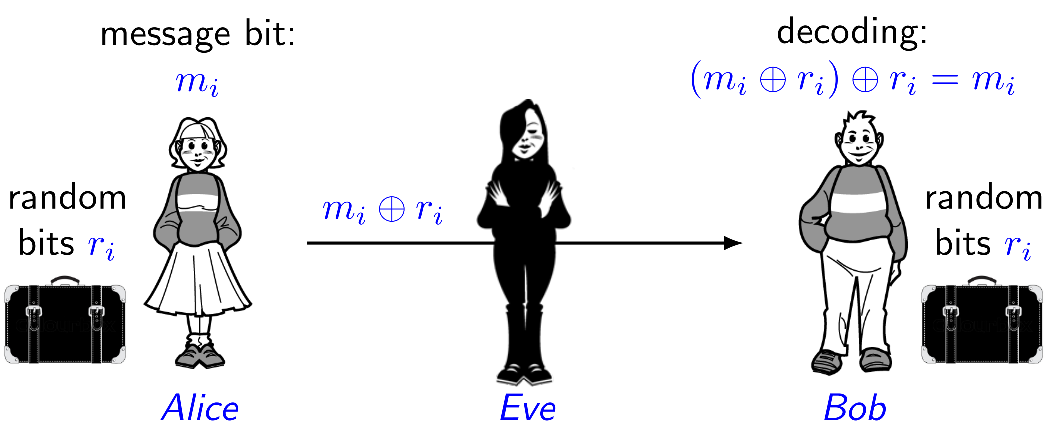
Currently running online course on *Quantum Cryptography*:
https://www.edx.org/course/quantum-cryptography-caltechx-delftx-qucryptox

One-time pad

Goal: Send a private message using public communication.
Protocol:

1. **Preparation:** *Alice* and *Bob* meet upfront to generate random bits $r_1, r_2, \ldots$ and both take a copy of these bits with them.
2. **Encoding:** If the i-th message bit is m_i, *Alice* sends $m_i \oplus r_i$.
3. **Decoding:** If *Bob* receives $\tilde{m}_i$, the actual message bit is $\tilde{m}_i \oplus r_i$.

Security: Eve gains no information about the message.



One-time pad

Resource trade-off: 1 shared random bit + 1 bit of public communication = 1 bit of private communication

Good:

- *Eve* gets no information about m_i as she observes a uniformly random bit (if r_i is uniform, then so is $m_i \oplus r_i$ irrespectively of m_i).
- One-time pad is unconditionally secure (there are no computational hardness assumptions).

Bad:

- The encryption key $r_1, r_2, \ldots$ is the same length as the message.
- The key cannot be replenished and should not be reused.
- How can *Alice* and *Bob* establish the key in the first place?

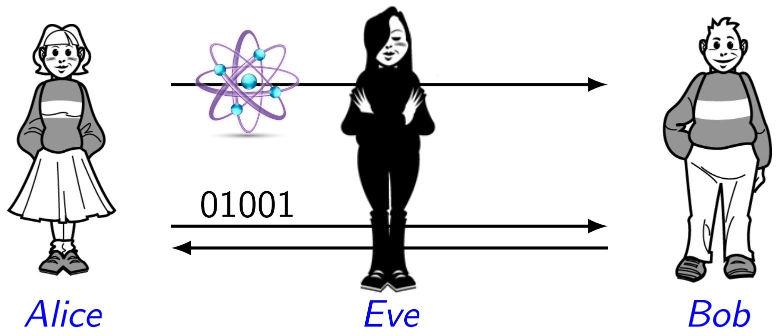
Quantum key distribution (QKD)

A quantum protocol for key distribution was invented by Bennett and Brassard in 1984 (it is known as BB84).

It provides means of establishing a private key—a random sequence of bits shared between *Alice* and *Bob* but unknown to any third party.

Later this key can be used in one-time pad to transmit a private message.

The protocol uses only public classical and quantum communication.



Key principle: Information gain implies disturbance!
(This is closely related to Heisenberg's uncertainty principle.)

Requirements for BB84

Public communication:

- *Alice* and *Bob* share a public authenticated classical channel.
- *Alice* can publicly send qubits to *Bob*.

Local operations:

- *Alice* has a private source of random classical bits.
- *Alice* can produce qubits in states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$.
- *Bob* can measure each of the incoming qubits in
  - either the standard basis $\{|0\rangle, |1\rangle\}$
  - or the Hadamard basis $\{|+\rangle, |-\rangle\}$.

Experimental implementations normally use polarised photons that are transmitted either through air or through optical fibre.

The BB84 rotocol

The basic BB84 protocol:

1. For $i = 1$ to n (below "$\in_R$" means "a random element of")
   - *Alice* picks $a_i \in_R \{0, 1\}$ and $U_i \in_R \{I, H\}$ and sends $U_i|a_i\rangle$ to *Bob*.
   - *Bob* guesses $V_i \in_R \{I, H\}$ and applies it on the received state.
   - *Bob* measures the resulting state $V_i U_i |a_i\rangle$ in the standard basis. We denote his measurement outcome by $b_i \in \{0, 1\}$.
2. *Bob* announces (over the public classical channel) which basis he used for each measurement (i.e., the string $V_1, \ldots, V_n$).
3. *Alice* announces $S \subseteq \{1, \ldots, n\}$ indicating which measurements where made in the correct basis.
4. Note that $a_i = b_i$ for all $i \in S$, so the shared key is $(a_i : i \in S)$.

	i	1	2	3	4	5	6	
Alice	$\|a_i\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	
	U_i	I	H	I	I	H	H	
	$U_i\|a_i\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\leftarrow$ public
Bob	V_i	H	H	I	H	I	H	$\leftarrow$ public
	$V_i U_i\|a_i\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$	
	$\|b_i\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	
Alice	S		✓	✓			✓	$\leftarrow$ public
Key			0	1			1	

Sanity checks

Why not announce the bases for all qubits before transmission, thus avoiding the loss of half the bits?

- This allows *Eve* to intercept, measure, and re-transmit the post-measurement state.

Why not announce the basis for each qubit after they are sent but before *Bob* measures them?

- Requires *Bob* to store the qubits (technologically difficult).
- If *Bob* can store them, so can *Eve*. She can perform the correct measurements and retransmit the post-measurement states to *Bob*.

Possible attacks

Could *Eve* intercept the qubits, re-transmit a copy to *Bob*, and then wait for the basis to be announced before measuring her own copy?

- **No-cloning theorem:** There is no unitary operation U such that $U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$ for all $|\psi\rangle$ simultaneously.

What if *Eve* intercepts the qubits, measures each one randomly in either the $\{|0\rangle, |1\rangle\}$ or the $\{|+\rangle, |-\rangle\}$ basis, and then retransmits them?

- Half of *Eve*'s measurements will be in the wrong basis.
- Moreover, these qubits will have changed state, so approximately $1/4$ of the final key bits of *Alice* and *Bob* will disagree.
- *Alice* and *Bob* can choose a random sample of their shared bits and publicly check their values against each other.
- If a large fraction disagrees (which could be either due to noise or due to an eavesdropper) they abort the protocol.
- **Information gain implies disturbance:** Measurements in the wrong basis cause disturbance that can be detected.

Extra post-processing

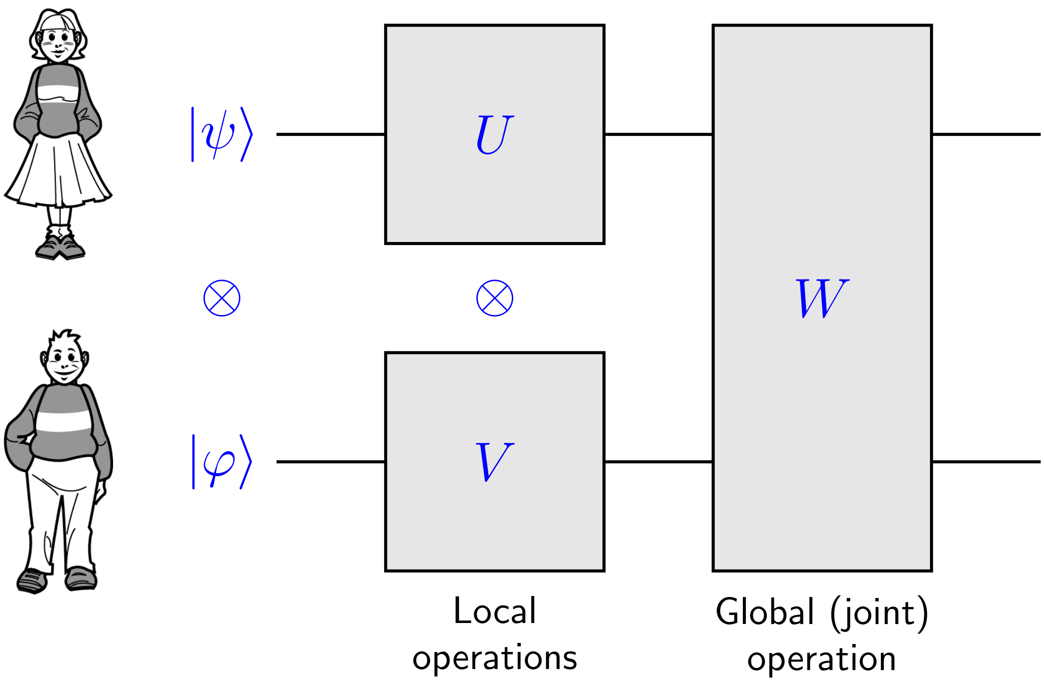
Ideal outcome: The strings of *Alice* and *Bob* are uniformly random, identical, and private from *Eve*.

More realistic: The strings might not agree either because of noise or because of *Eve*.

Extra steps:

- Information reconciliation: a form of error correction that ensures the keys shared by *Alice* and *Bob* are identical.
- Privacy Amplification: eliminates any partial information *Eve* might have about the key shared by *Alice* and *Bob*.

Local vs global operations



Remember: Local unitary operations cannot produce or destroy entanglement, only global operations can! Local measurements can only destroy entanglement.

Bell states

Entanglement-based protocols generally rely on using the following four states of a two-qubit system, known as the Bell states:

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \qquad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

They form an orthonormal basis for $\mathbb{C}^4$, known as the Bell basis.
An orthogonal measurement in this basis is called Bell measurement.

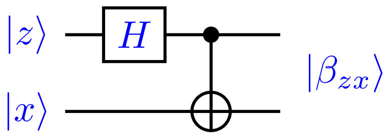
These states can be written concisely as follows ($\bar{x} \equiv x \oplus 1$):

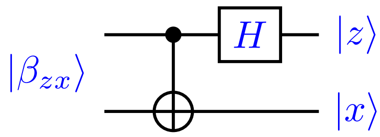
$$|\beta_{zx}\rangle = \frac{1}{\sqrt{2}}(|0, x\rangle + (-1)^z|1, \bar{x}\rangle)$$

Note that, in each of the states, measuring either qubit in the computational basis yields $|0\rangle$ or $|1\rangle$ with equal probability, and after the measurement, the other bit is uniquely determined.

Properties of Bell states

Preparation / unpreparation: A global unitary can generate the Bell states from the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ and vice versa:





$|\beta_{zx}\rangle = \mathrm{CNOT} \cdot (H \otimes I) \cdot |z, x\rangle$ $\qquad$ $|z, x\rangle = (H \otimes I) \cdot \mathrm{CNOT} \cdot |\beta_{zx}\rangle$

Local conversion: Any Bell state can be converted into any other by either of the two parties using only local (Pauli) unitaries:

$$|\beta_{zx}\rangle = (Z^z X^x \otimes I) \cdot |\beta_{00}\rangle = (I \otimes X^x Z^z) \cdot |\beta_{00}\rangle$$

The state $|\beta_{00}\rangle$ is often called EPR pair (for Einstein–Podolsky–Rosen).

Superdense coding: sanity check

Goal: Send two classical bits by transmitting one qubit.

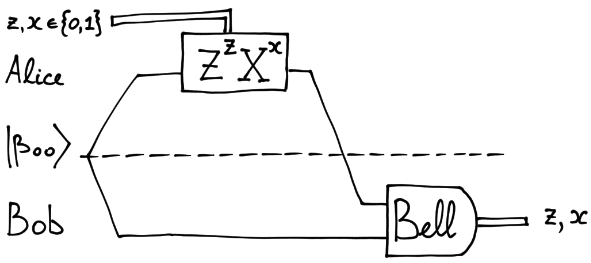
Holevo's theorem: It is impossible to encode more than one classical bit of information in a single isolated qubit and then recover it reliably.

Resolution: Superdense coding does not contradict this fact, since it does not use an isolated qubit (i.e., a qubit that is in a product state with the receiver). At the beginning of the protocol, *Alice* and *Bob* share the EPR state $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ which is entangled.

Main idea: *Alice* can locally convert $|\beta_{00}\rangle$ to any other Bell state $|\beta_{zx}\rangle$ by performing an operation just on her own qubit. Once her qubit is sent to *Bob*, it reliably conveys two bits of classical information since the four Bell states are orthonormal.

Superdense coding

If *Alice* shares an EPR state $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with *Bob*, she can locally transform it to any other EPR state $|\beta_{zx}\rangle$ by applying $Z^z X^x$ on her qubit. In this way she can encode two bits $z, x \in \{0, 1\}$ in one of the four orthogonal Bell states $|\beta_{zx}\rangle$. If *Alice* sends her qubit to *Bob*, he can perfectly discriminate the four cases by measuring in the Bell basis:



$$(H \otimes I) \cdot \mathrm{CNOT} \cdot (Z^z X^x \otimes I) \cdot |\beta_{00}\rangle = |z, x\rangle$$

Resource trade-off: 1 shared EPR state + 1 qubit of quantum communication = 2 bits of classical communication

Teleportation vs superdense coding

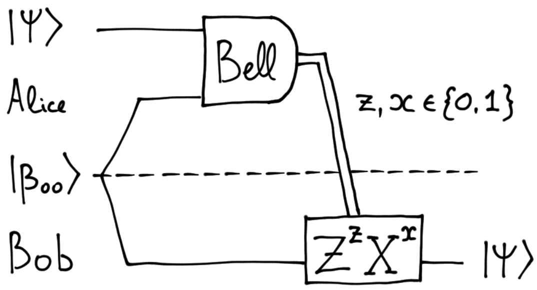
Superdense coding and quantum teleportation are dual to each other. By consuming one copy of a shared EPR state,

- the superdense coding protocol allows *Alice* to send *Bob* two classical bits by transmitting a single qubit,
- the quantum teleportation protocol allows *Alice* to send *Bob* a qubit, by transmitting just two classical bits.

Note: Teleportation does not violate the no-cloning theorem since *Alice*'s copy of the state is destroyed in the process.

Quantum teleportation

Alice has a state $|\psi\rangle$ that she wishes to transmit to *Bob* with whom she shares an EPR state $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. *Alice* measures her qubits in the Bell basis and sends the classical outcomes $z, x \in \{0,1\}$ to *Bob* who applies the Pauli correction operation $Z^z X^x$ on his qubit:



$$|\psi\rangle \otimes |\beta_{00}\rangle = \frac{1}{2} \sum_{z,x\in\{0,1\}} |\beta_{zx}\rangle \otimes X^x Z^z |\psi\rangle$$

Resource trade-off: 1 shared EPR state + 2 bits of classical communication = 1 qubit of quantum communication

Summary

- **One-time pad:** $(m_i \oplus r_i) \oplus r_i = m_i$
- **BB84:** *Alice* sends a random state from $\{|0\rangle, |0\rangle, |+\rangle, |-\rangle\}$, *Bob* tries to guess the correct basis; each correct guess gives on bit of key
- **Local vs global:** $U \otimes V$ is local and cannot create entanglement; non-product unitaries are global and they can create entanglement; by transmitting qubits from one party to the other, global operations can be performed locally
- **Bell states:** $|\beta_{zx}\rangle = \frac{1}{\sqrt{2}}(|0, x\rangle + (-1)^z |1, \bar{x}\rangle)$ are orthonormal and locally convertible to each other

Resource trade-offs:

- **One-time pad:** 1 shared random bit + 1 bit of public communication = 1 bit of private communication
- **Superdense coding:** 1 shared EPR state + 1 qubit of quantum communication = 2 bits of classical communication
- **Quantum teleportation:** 1 shared EPR state + 2 bits of classical communication = 1 qubit of quantum communication