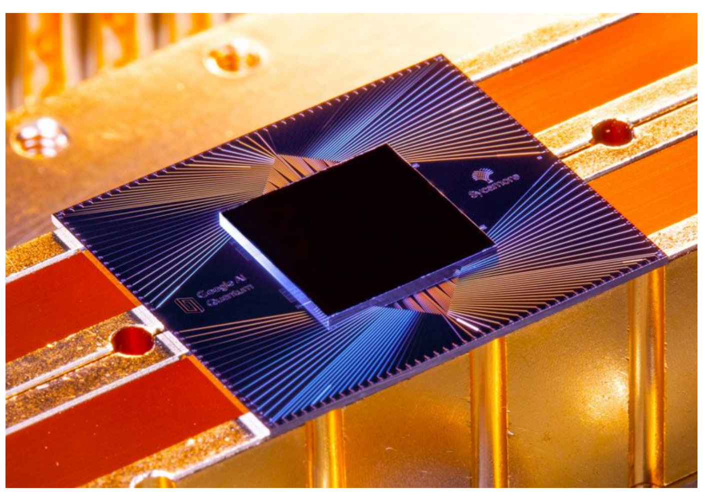
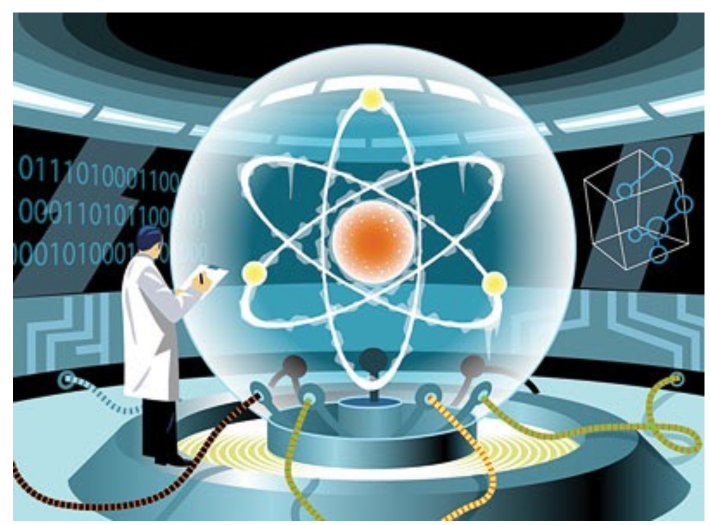
9th NCCR QSIT Winter School

# Quantum Information Theory

Joseph M. Renes
ETH Zürich

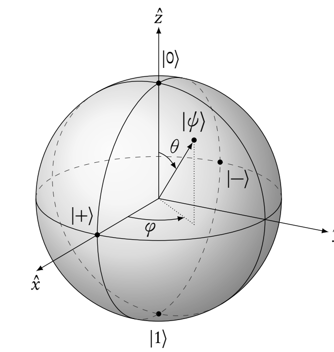
# What is quantum information theory?
# What is it good for?

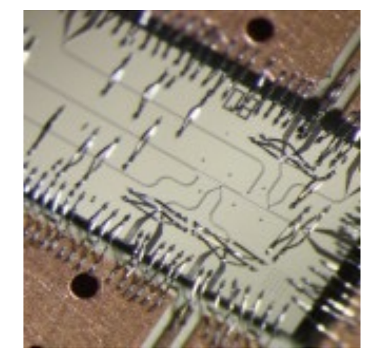



# Outline

- Concepts: Information & Quantum
- Mathematical setting: Qubits 1,2,3

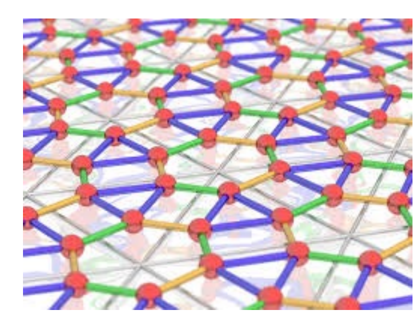



- Application: Quantum Computing



- Application: Quantum Crypto

- Challenges of Quantum Information Processing



# Concepts: Information & Quantum

## What is information?

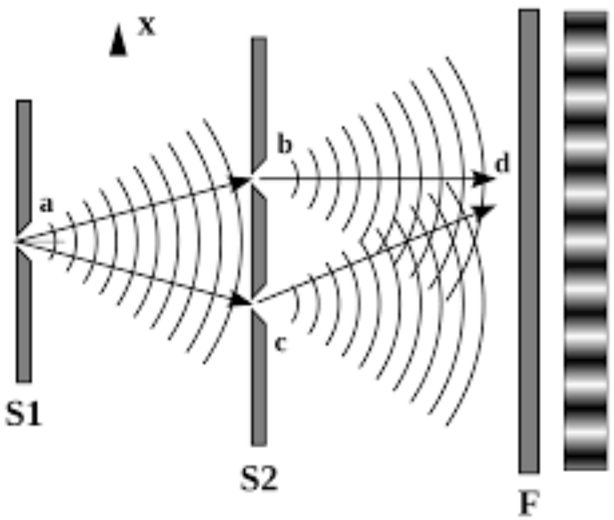

- Wiener: “Because information depends, not merely on what is actually said, but on what *might have been said*, its measure is a property of *a set of* possible messages…”
- Amount of information: *number* of messages.
  Count logarithmically: measure in *bits*.
- Information processor: manipulate *possible symbols*
  (don’t care how they are physically manifested)

Is this an information processor?

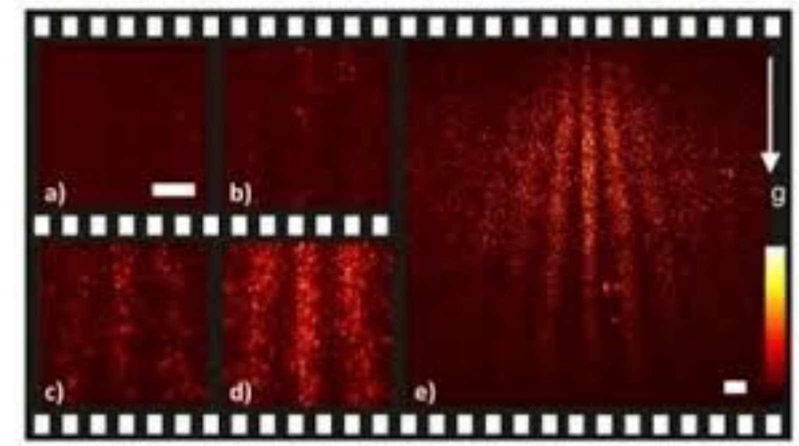
There's only one message. (need butter)

What about:

# Concepts: Information & Quantum




What is quantum?





Consider superposition of symbols

Quantum Information Processing:
manipulating superpositions of symbols

Quantum: need to use quantum statistical description;
*not* that QM is required to describe physical device

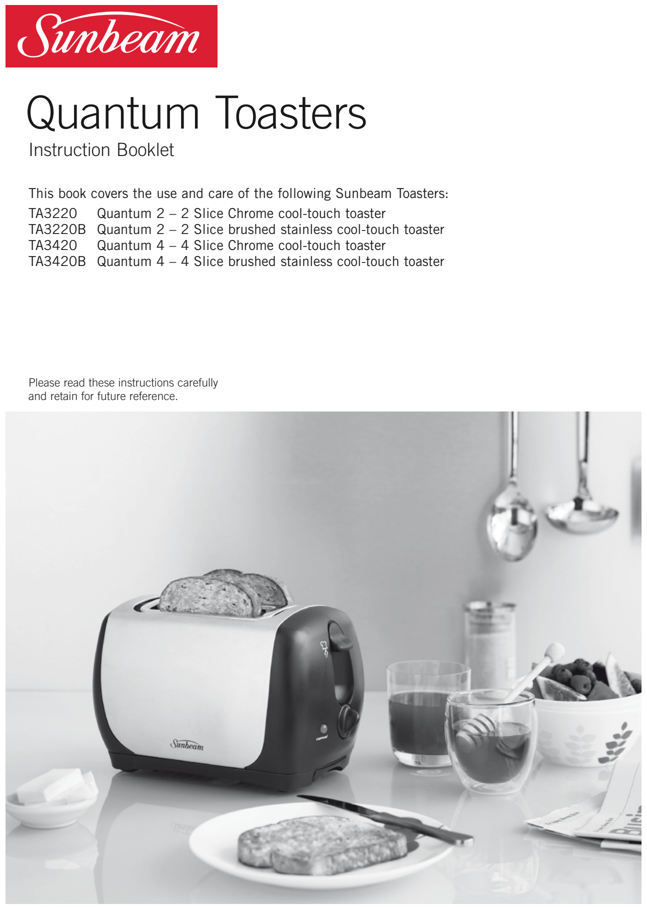
Superposition invalidates *counterfactual reasoning:*
e.g. what might have been said

We know this because of experimental
loophole-free Bell inequality violations:

"Unperformed experiments have no results"
—Asher Peres

Trouble for *quantum* information processing?

# Focus on devices, not experiments

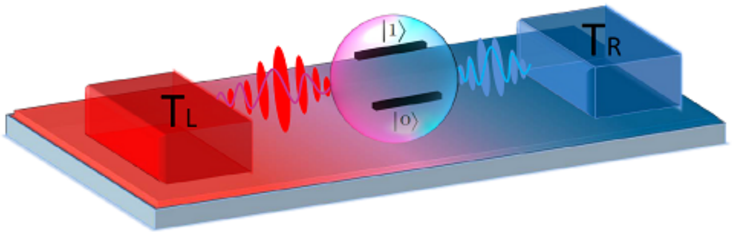




Cloning

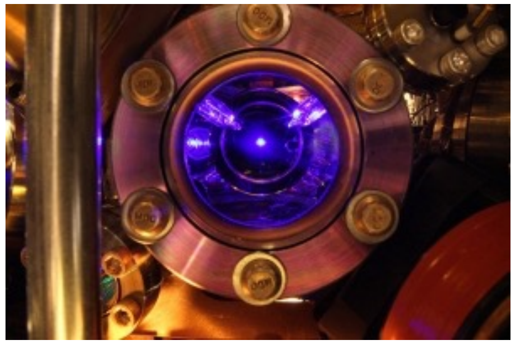
No machine can copy every possible quantum message

But any given state can be cloned

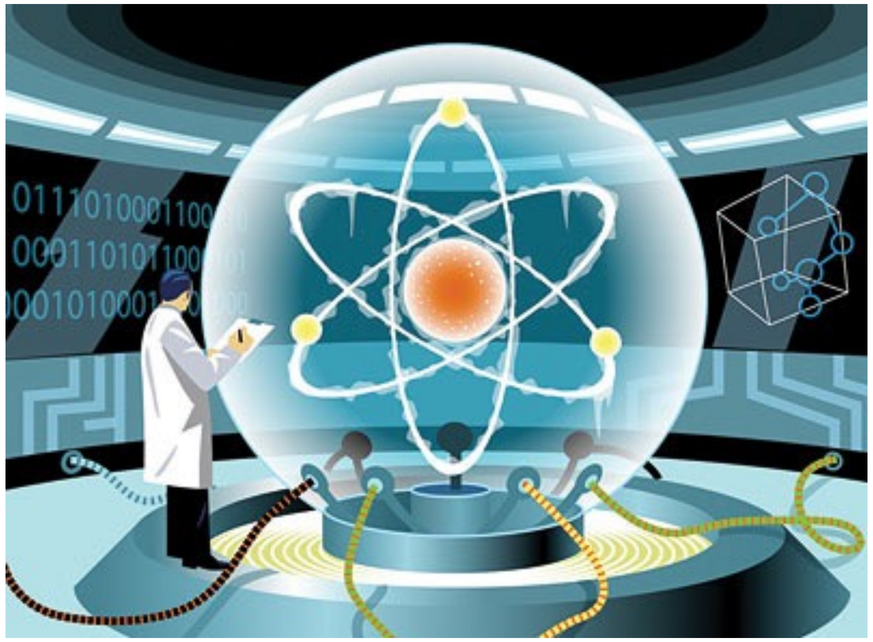



Thermo

Crypto

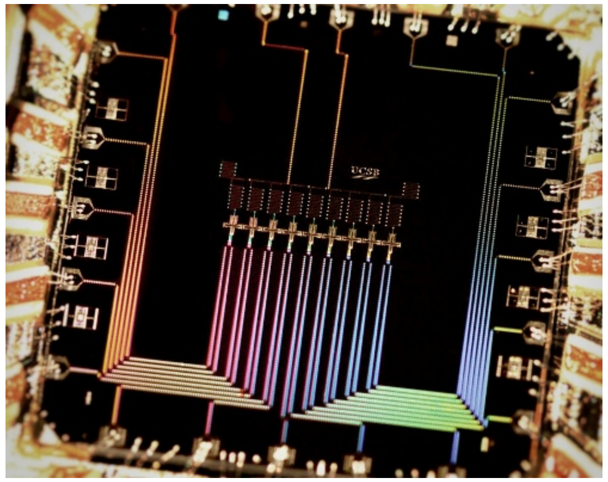


Metrology

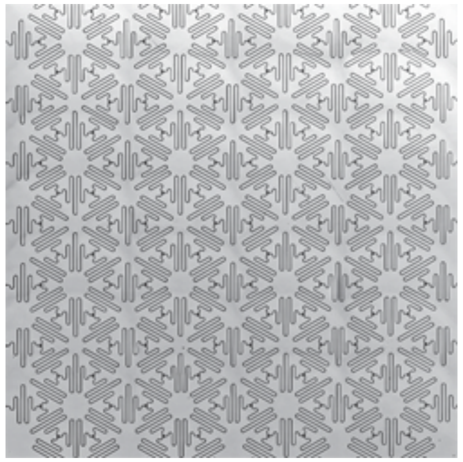


Applications

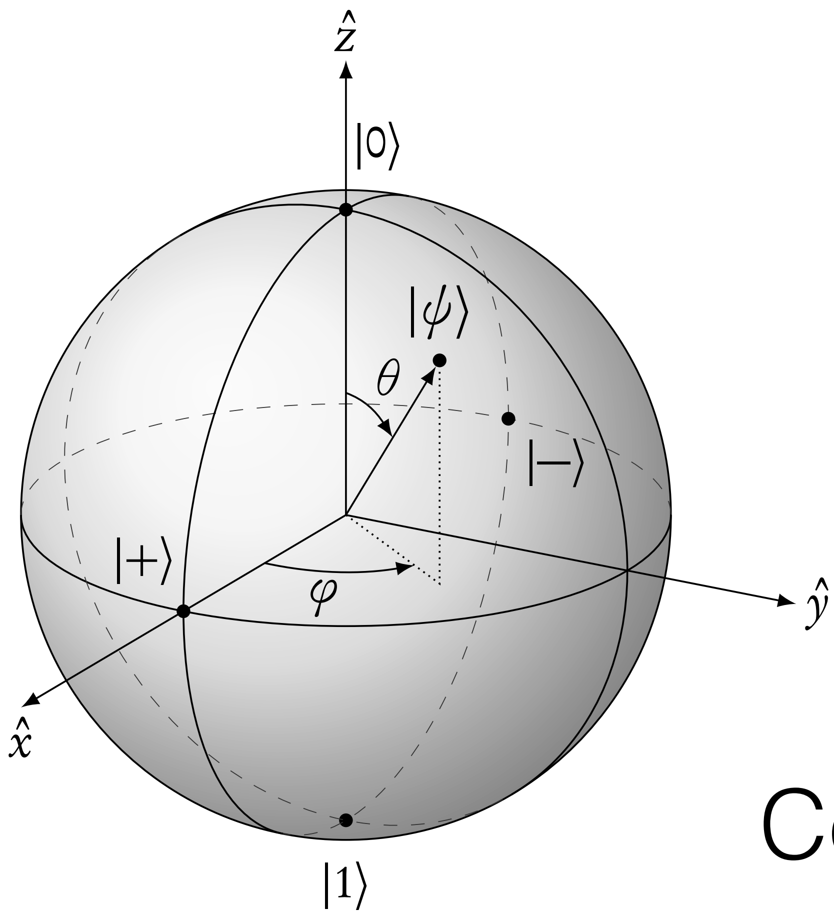
Communication



Computing



Quantum Simulation




# Qubits

spins, polarization, ground/excited, etc.

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

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in \mathbb{C}^2$$

Coherent: test interference of 0 and 1

1. Prepare qubit states

2. Rotate qubit states:
unitary dynamics (Schrödinger equation)

3. Measure them: $\Pr(0)_{|\psi\rangle} = |\langle 0|\psi\rangle|^2$

$$\Pr(0)_{|+\rangle} = |\langle 0|+\rangle|^2 = \frac{1}{2}$$


# Many Qubits

basis: sequence of bits

$$|0\rangle_A \otimes |0\rangle_B \otimes |1\rangle_C$$

And superpositions:

$$|0\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C + |1\rangle_A \otimes |1\rangle_B \otimes |1\rangle_C$$

Abbreviate: $|000\rangle_{ABC} + |111\rangle_{ABC}$

Entanglement: superposition of many qubit state

$$|0\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C + |1\rangle_A \otimes |1\rangle_B \otimes |1\rangle_C$$

No cloning argument:

No machine can copy every input state

$$M(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$$

M is described by a unitary operator: *linear*

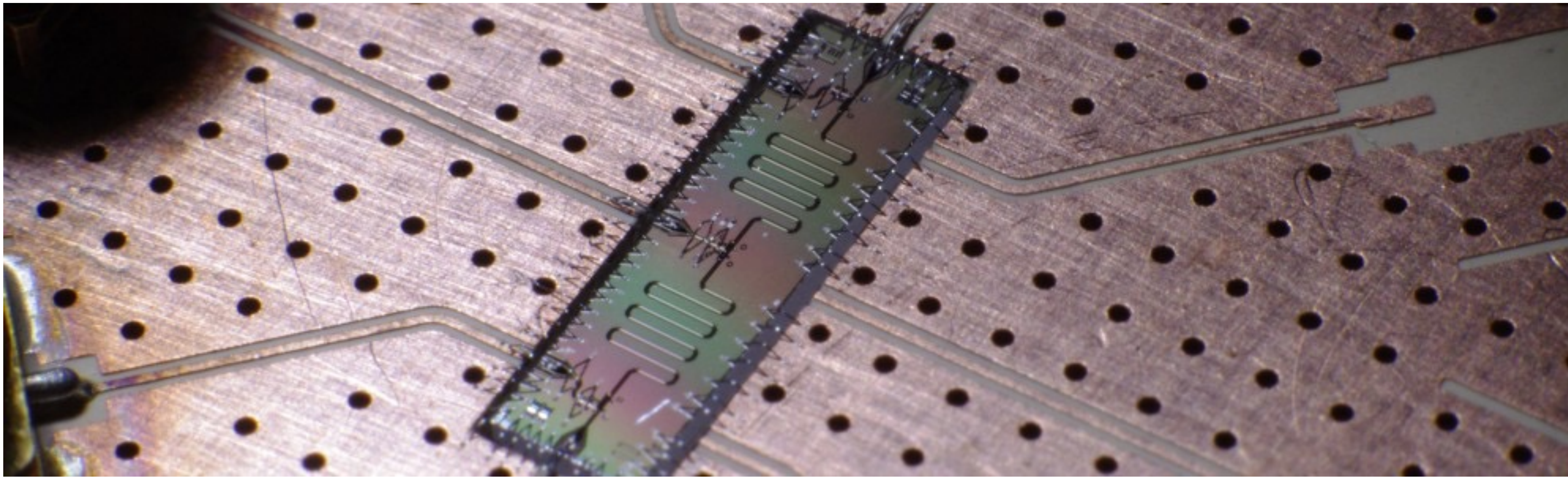
$$U_M|\psi\rangle \otimes |0\rangle = \alpha U_M|0\rangle \otimes |0\rangle + \beta U_M|1\rangle \otimes |0\rangle$$

Suppose it works for 0, 1:

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

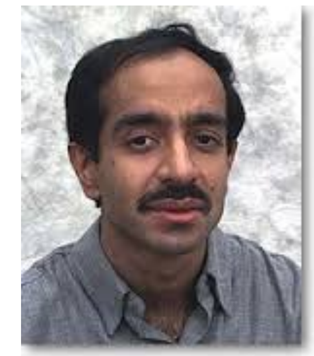
$$\neq |\psi\rangle \otimes |\psi\rangle$$

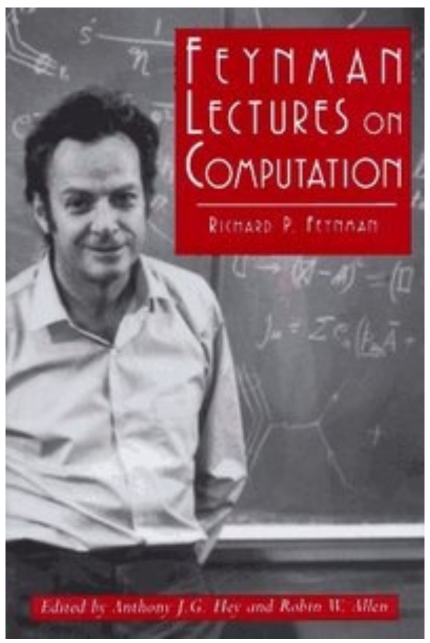
Application:



Computing

Famously: efficient factoring, searching



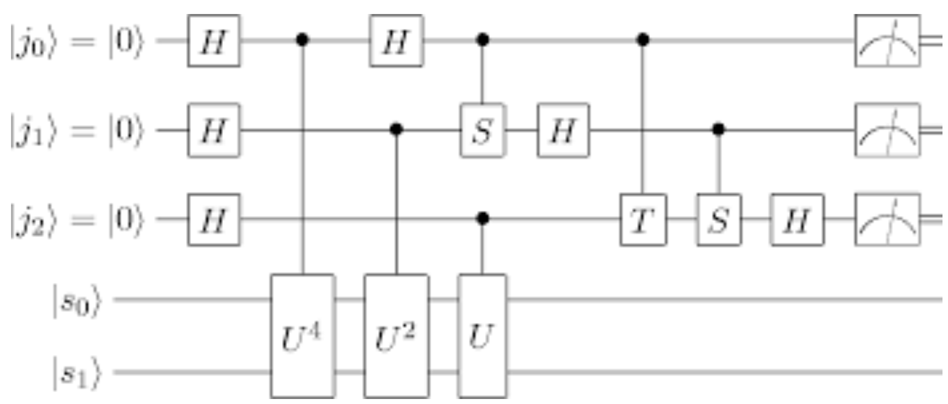



Also: might like to
simulate quantum systems

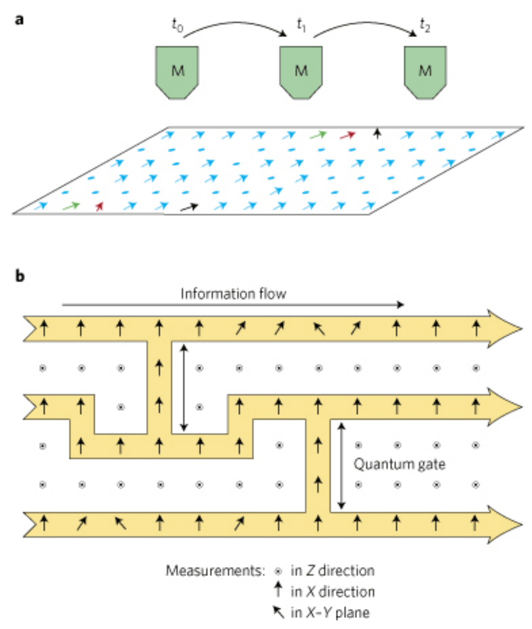
Task is the same: classical input, classical output
But with favorable scaling

# Computing models

Circuit model: qubit memory + gates



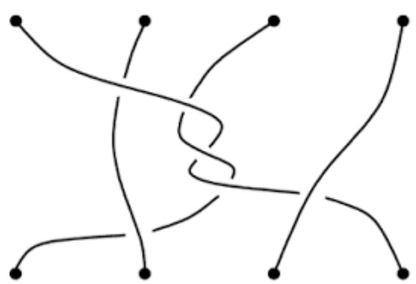

Measurement-based:




make cluster state + measure

Adiabatic:

1. start in ground state of simple Hamiltonian
2. slowly change to final Hamiltonian
3. ground state encodes solution of the problem



Topological:
qubits are ground state degen. of QFT
manipulate excitations to perform gates

Efficiency: How many steps in circuit? How slow an adiabatic process?

Deutsch-Jozsa

1-bit function f:
balanced or constant?

identity, NOT

$f(0) \neq f(1)$

output 0 or 1

$f(0) = f(1)$

Classically: Need two queries to f

Quantumly: Just one!

Quantum query: $|x\rangle|y\rangle \xrightarrow{U_f} |x\rangle|y \oplus f(x)\rangle$

Q: What happens if superpose the target?

A: Phase kickback $$|x\rangle|-\rangle \xrightarrow{U_f} (-1)^{f(x)}|x\rangle|-\rangle$$

the effect of the function f is purely in the phase

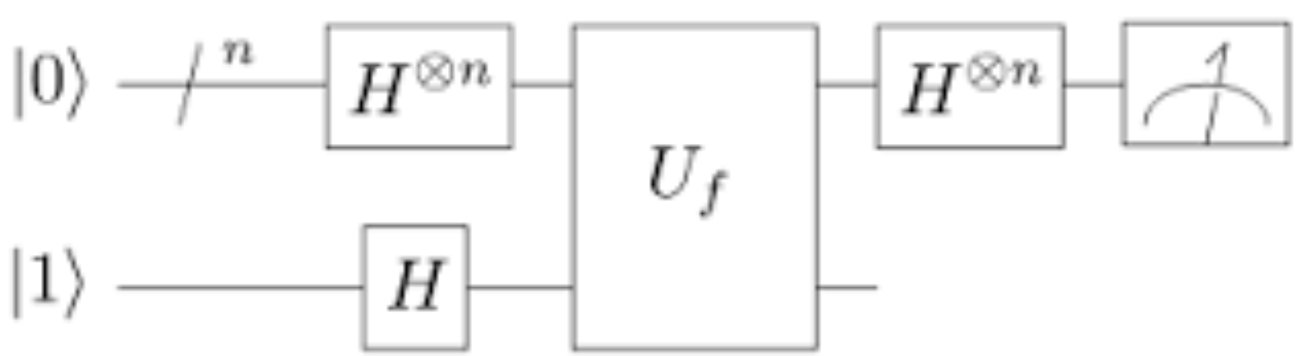
Proof: $$|x\rangle(|0\rangle - |1\rangle) \xrightarrow{U_f} |x\rangle|f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle$$

Now superpose the controls: Query in superposition!

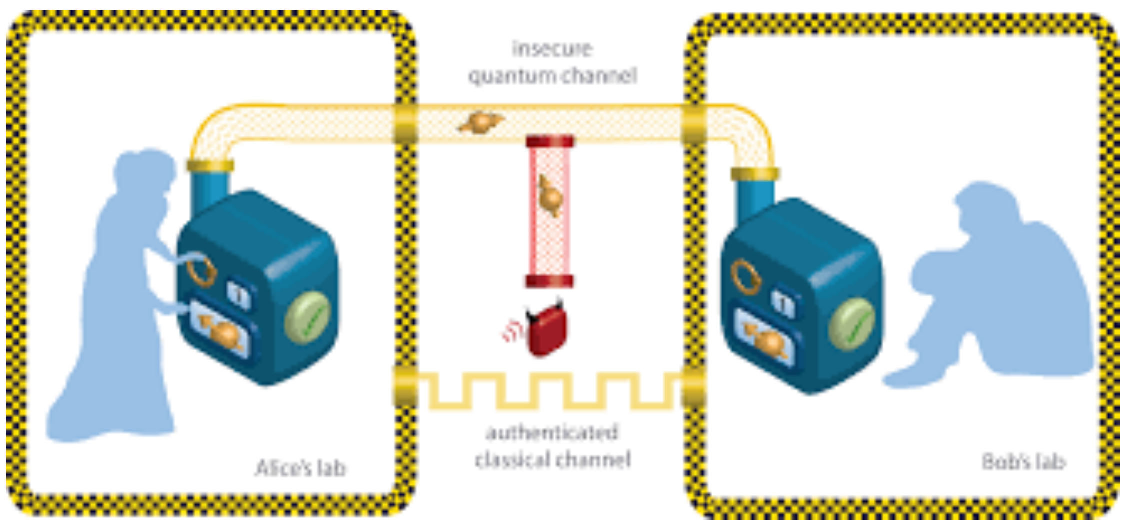
$$|+\rangle|-\rangle \xrightarrow{U_f} \sum_{x=0}^{1}(-1)^{f(x)}|x\rangle|-\rangle$$

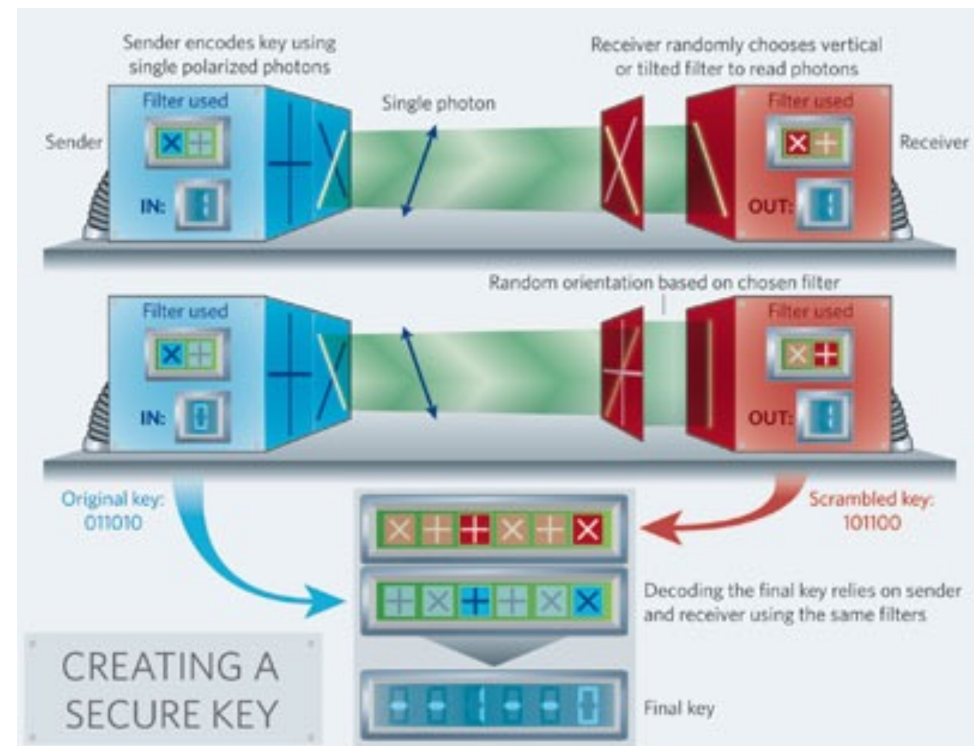
$|+\rangle|-\rangle$ if constant

$|-\rangle|-\rangle$ if balanced



# Application:



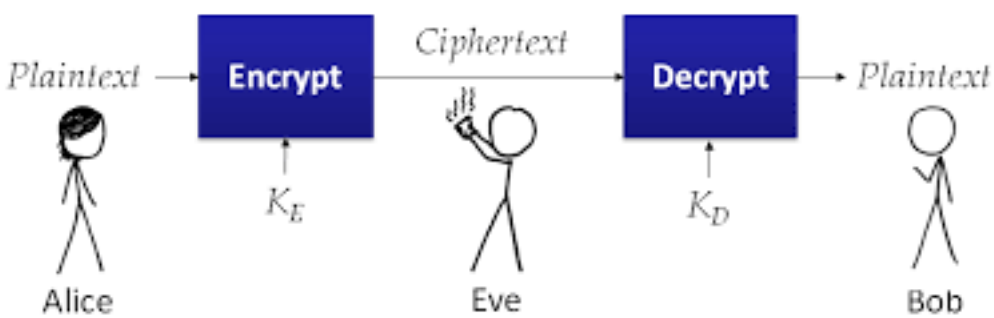

# Cryptography

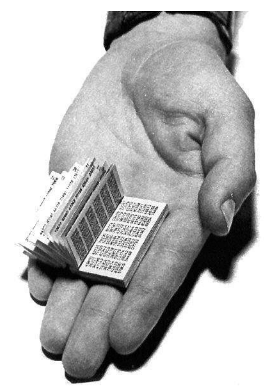
Want: *private* communication between Alice and Bob
Have: *insecure* classical and quantum channels

????

Focus on creating *secret key* for *one-time pad.*

Problem is “solved” if Alice and Bob share a secret key



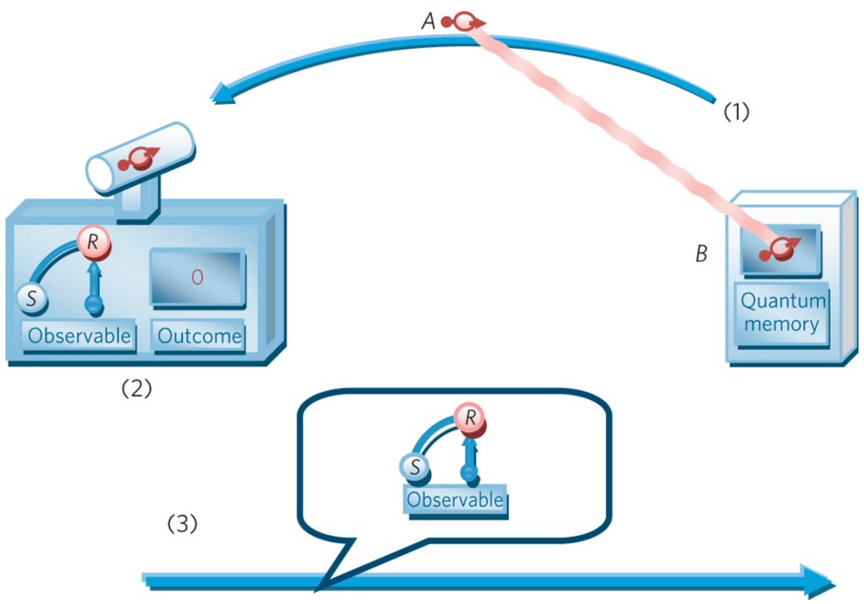
one-time pad:
random key symbol for
every message symbol

```
       H       E       L       L       O   message
    7 (H)   4 (E)  11 (L)  11 (L)  14 (O)  message
+  23 (X)  12 (M)   2 (C)  10 (K)  11 (L)  key
=  30      16      13      21      25      message + key
=   4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z)  message + key (mod 26)
       E       Q       N       V       Z   → ciphertext
```

```
       E       Q       N       V       Z   ciphertext
    4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z)  ciphertext
–  23 (X)  12 (M)   2 (C)  10 (K)  11 (L)  key
= -19       4      11      11      14      ciphertext – key
=   7 (H)   4 (E)  11 (L)  11 (L)  14 (O)  ciphertext – key (mod 26)
       H       E       L       L       O   → message
```

Great! All we need is the key. ????

Classically: Catch-22
Quantumly: Use the uncertainty principle!




"But you can't go through life applying Heisenberg's Uncertainty Principle to everything."

# Uncertainty games

Alice makes one of two complementary measurements; Bob tries to guess.

## Version A

1. Bob prepares qubit, sends to Alice
2. Bob makes a guess for *each* measurement
3. Alice randomly measures, tells Bob.

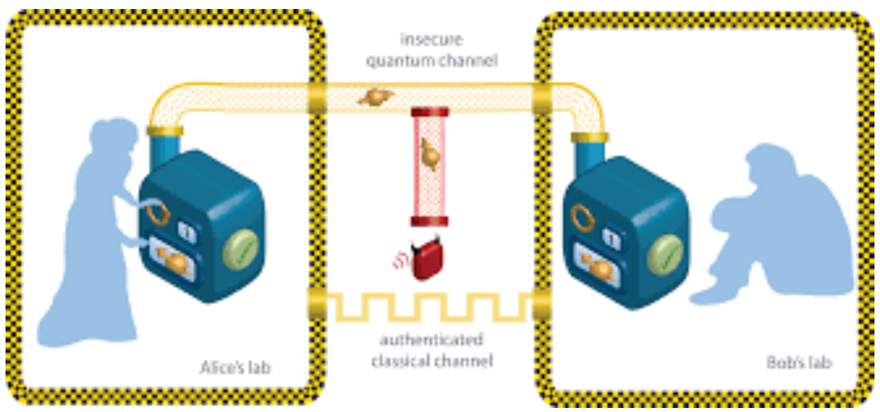
Cannot win:
like predicting position and momentum

## Version B

1. Bob prepares qubit, sends to Alice
2. Alice commits to one measurement,
3. Alice asks for guess, Bob delivers.
4. Alice measures, tells Bob.

Can win:
prepare entangled state,
keep half & measure appropriately

1. Alice prepares entangled state, sends half to Bob. (repeat x zillion)
2. A+B compare some qubits. Alice measures X or Z, Bob guesses
3. If guesses are good, use remaining qubits for key via X/Z meas.

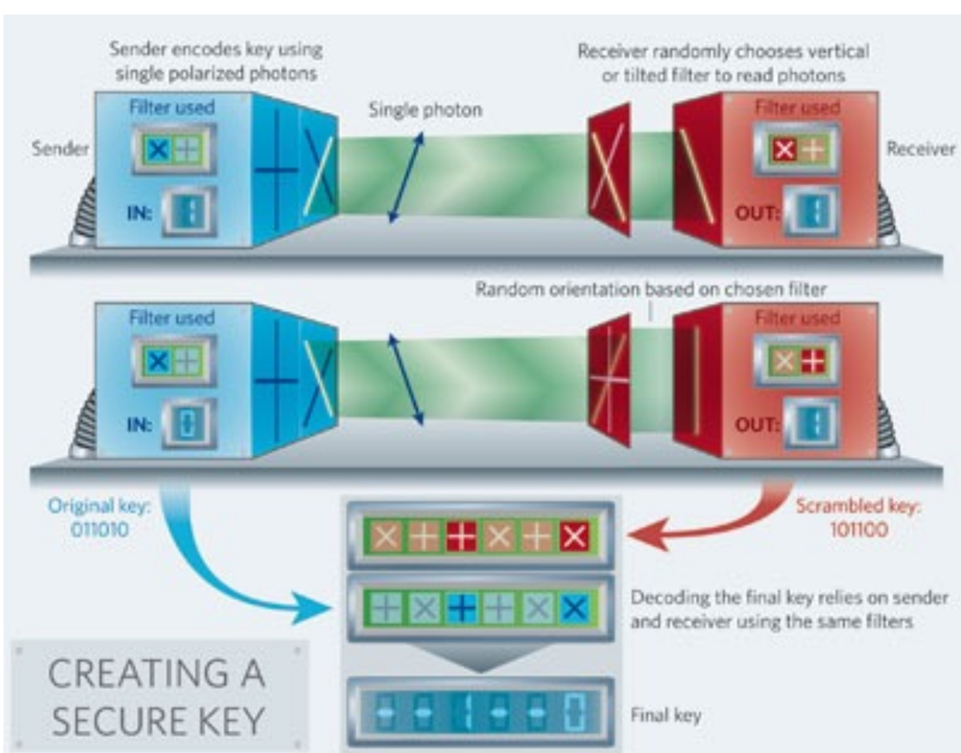



Resulting key is private. Why?

If guesses are good, AB state is entangled: $|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B$

(ver. B)

Consider a remaining qubit pair: Alice measures Z to create key. Bob could have predicted X, so Eve cannot predict Z. (ver. A)

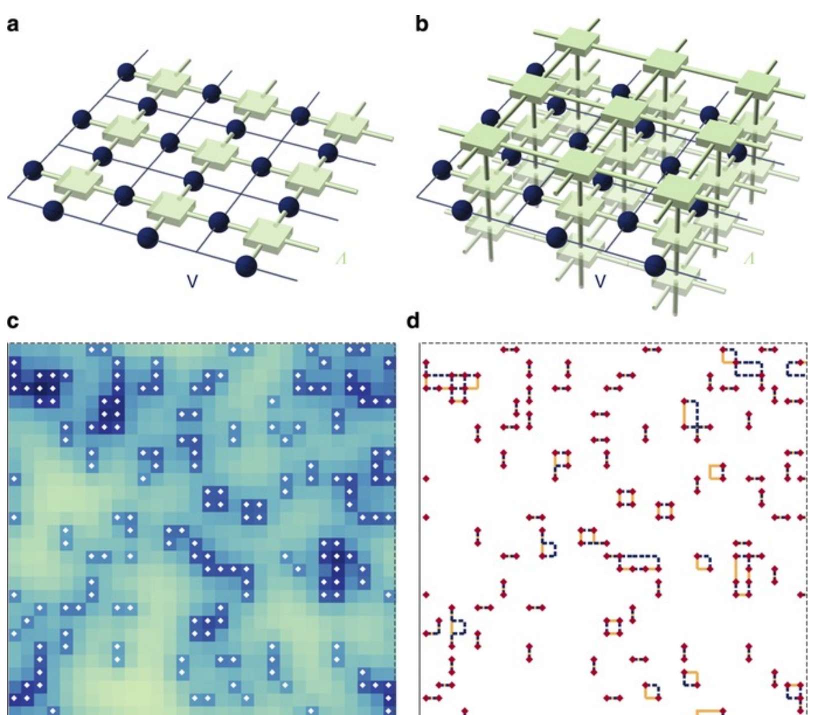



Can convert to “prepare & measure” scheme: BB84

Blackbox: Statistics same

# Challenges of Quantum Information Processing


Noise!




Error correction
Fault tolerance