Quantum Computing

Ronald de Wolf

CWI

QuSoft

Universiteit van Amsterdam

Quantum-mechanical computers

Quantum-mechanical computers

- Our society runs on classical computers

Quantum-mechanical computers

- Our society runs on classical computers:
  memory-locations have specific value (0 or 1),
  processor acts on specific location, ...

Quantum-mechanical computers

- Our society runs on classical computers: memory-locations have specific value (0 or 1), processor acts on specific location, ...
- But our world is not classical, so let's study quantum-mechanical computers

Quantum-mechanical computers

- Our society runs on classical computers: memory-locations have specific value (0 or 1), processor acts on specific location, ...
- But our world is not classical, so let's study quantum-mechanical computers
- Why?
  1. Enable further miniaturization (Moore's law)

Quantum-mechanical computers

- Our society runs on classical computers: memory-locations have specific value (0 or 1), processor acts on specific location, ...
- But our world is not classical, so let's study quantum-mechanical computers
- Why?
  1. Enable further miniaturization (Moore's law)
  2. Enable large speed-up for some important problems

Quantum-mechanical computers

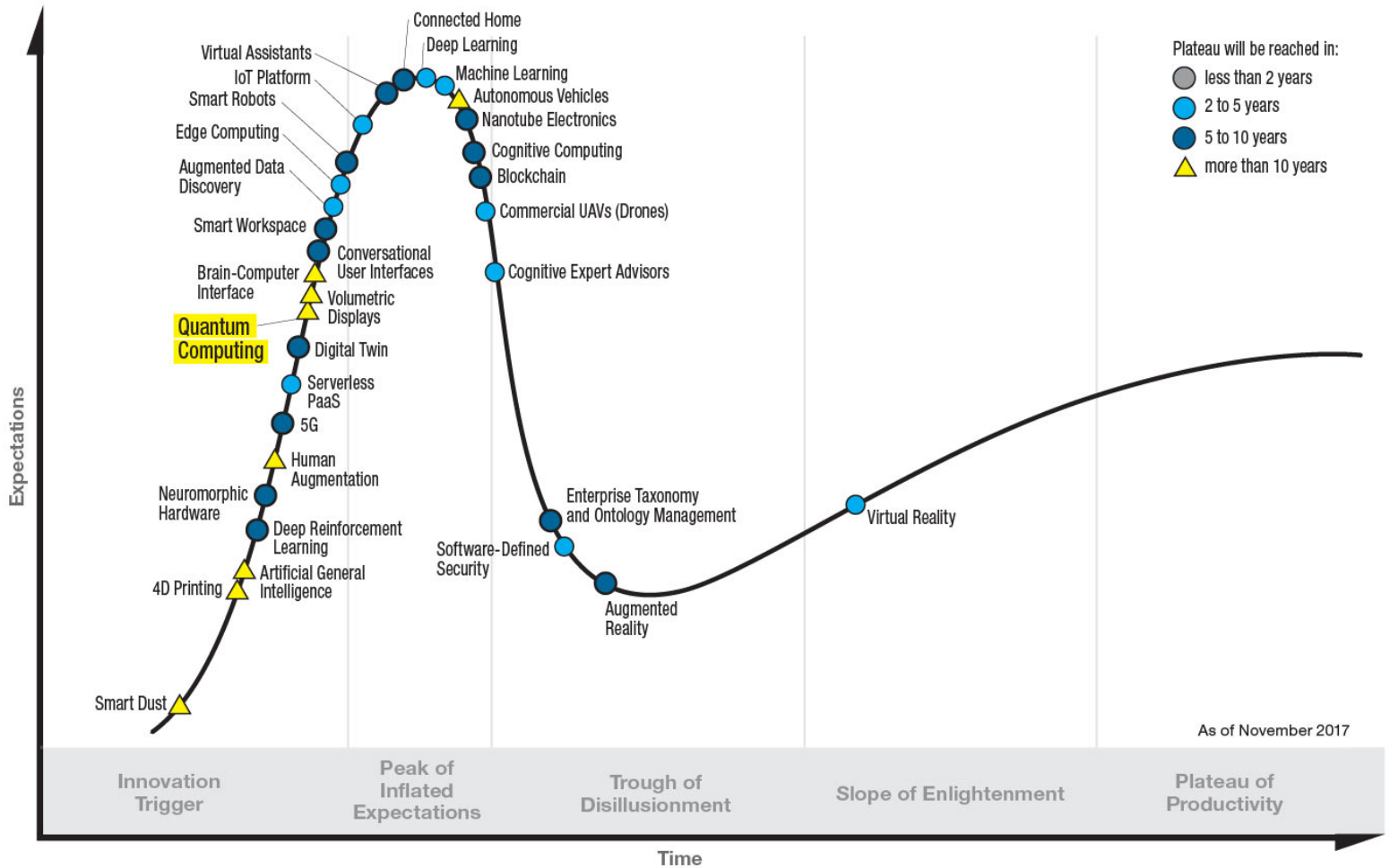
- Our society runs on classical computers:
  memory-locations have specific value (0 or 1),
  processor acts on specific location, ...

- But our world is not classical, so let's study
  quantum-mechanical computers

- Why?

  1. Enable further miniaturization (Moore's law)
  2. Enable large speed-up for some important problems
  3. The goal of computer science is to study the power
     of the best computing machines that Nature allows us

Gartner Hype Cycle for Emerging Technologies



gartner.com/SmarterWithGartner

Source: Gartner (November 2017)

Gartner

Quantum computers: hype vs substance

The goal of this talk:

Assume large quantum computers will be built in the next decades.

Where will they have a real impact?

Quantum computers: hype vs substance

The goal of this talk:

Assume large quantum computers will be built in the next decades.

Where will they have a real impact?

- Probably: Cryptography, optimization, simulation

Quantum computers: hype vs substance

The goal of this talk:

Assume large quantum computers will be built in the next decades.

Where will they have a real impact?

- Probably: Cryptography, optimization, simulation
- Maybe: Machine learning

Quantum computers: hype vs substance

The goal of this talk:

Assume large quantum computers will be built in the next decades.

Where will they have a real impact?

- Probably: Cryptography, optimization, simulation
- Maybe: Machine learning
- Forget about it: NP-hard problems (TSP, protein folding,...)

Quantum computers: hype vs substance

The goal of this talk:

Assume large quantum computers will be built in the next decades.

Where will they have a real impact?

- Probably: Cryptography, optimization, simulation
- Maybe: Machine learning
- Forget about it: NP-hard problems (TSP, protein folding,...), ending climate change, finding ET, ...

Quantum bits

Quantum bits

- A classical bit is 0 or 1

Quantum bits

- A classical bit is 0 or 1
- Quantum mechanics allows superposition of $|0\rangle$ and $|1\rangle$, each with its own "amplitude"

Quantum bits

- A classical bit is 0 or 1
- Quantum mechanics allows superposition of $|0\rangle$ and $|1\rangle$, each with its own "amplitude". This is a qubit

Quantum bits

- A classical bit is 0 or 1
- Quantum mechanics allows superposition of $|0\rangle$ and $|1\rangle$, each with its own "amplitude". This is a qubit
- We can use any physical system with two distinguishable basis states to build a qubit:

Quantum bits

- A classical bit is 0 or 1
- Quantum mechanics allows superposition of $|0\rangle$ and $|1\rangle$, each with its own "amplitude". This is a qubit
- We can use any physical system with two distinguishable basis states to build a qubit:

  electron spin

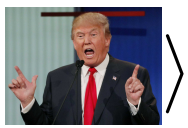
Quantum bits

- A classical bit is 0 or 1
- Quantum mechanics allows superposition of $|0\rangle$ and $|1\rangle$, each with its own "amplitude". This is a qubit
- We can use any physical system with two distinguishable basis states to build a qubit:

  electron spin, photon polarization

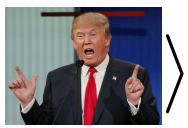
Quantum bits

- A classical bit is 0 or 1
- Quantum mechanics allows superposition of $|0\rangle$ and $|1\rangle$, each with its own "amplitude". This is a qubit
- We can use any physical system with two distinguishable basis states to build a qubit:

  electron spin, photon polarization, $|$  $\rangle + |$  $\rangle$

Quantum bits

- A classical bit is 0 or 1
- Quantum mechanics allows superposition of $|0\rangle$ and $|1\rangle$, each with its own "amplitude". This is a qubit
- We can use any physical system with two distinguishable basis states to build a qubit:

  electron spin, photon polarization, $|$  $\rangle + |$  $\rangle$

- 2 qubits: superposition of 4 possible basis states (00,01,10,11)

Quantum bits

- A classical bit is 0 or 1
- Quantum mechanics allows superposition of $|0\rangle$ and $|1\rangle$, each with its own "amplitude". This is a qubit
- We can use any physical system with two distinguishable basis states to build a qubit:

  electron spin, photon polarization, $|$  $\rangle + |$  $\rangle$

- 2 qubits: superposition of 4 possible basis states (00,01,10,11)

  3 qubits: superposition of 8 possible basis states

Quantum bits

- A classical bit is 0 or 1
- Quantum mechanics allows superposition of $|0\rangle$ and $|1\rangle$, each with its own "amplitude". This is a qubit
- We can use any physical system with two distinguishable basis states to build a qubit:

  electron spin, photon polarization, $|$  $\rangle + |$  $\rangle$

- 2 qubits: superposition of 4 possible basis states (00,01,10,11)

  3 qubits: superposition of 8 possible basis states

  $\vdots$

  n qubits: superposition of 2^n possible basis states

Quantum bits

- A classical bit is 0 or 1
- Quantum mechanics allows superposition of $|0\rangle$ and $|1\rangle$, each with its own "amplitude". This is a qubit
- We can use any physical system with two distinguishable basis states to build a qubit:

  electron spin, photon polarization, $|$  $\rangle + |$  $\rangle$

- 2 qubits: superposition of 4 possible basis states (00,01,10,11)

  3 qubits: superposition of 8 possible basis states

  $\vdots$

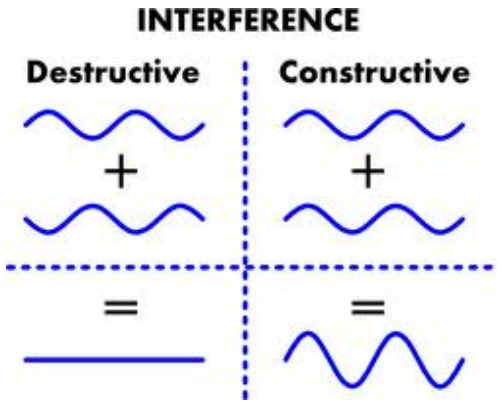
  n qubits: superposition of 2^n possible basis states

  Described by a "wavefunction": vector of all 2^n amplitudes

Quantum computers in a nutshell

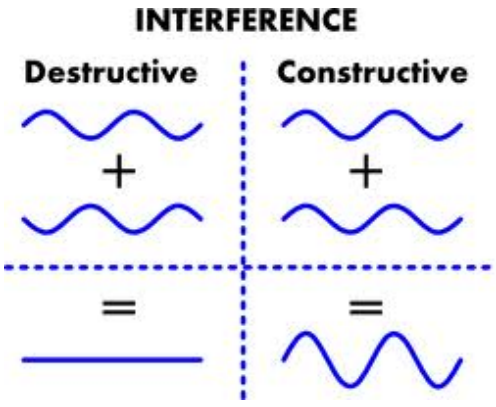
Quantum computers in a nutshell

- Waves can strengthen or weaken each other:



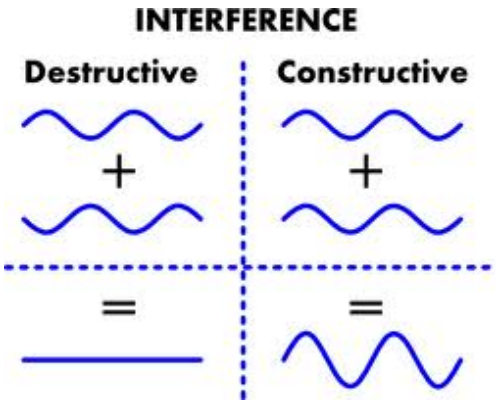
Quantum computers in a nutshell

- Waves can strengthen or weaken each other:



Quantum computers in a nutshell

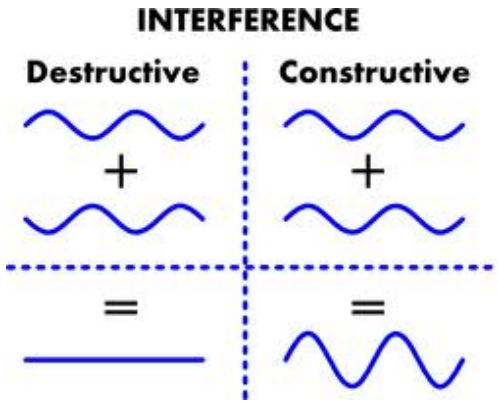
- Waves can strengthen or weaken each other:



- Quantum computation = superposition + interference

Quantum computers in a nutshell

- Waves can strengthen or weaken each other:

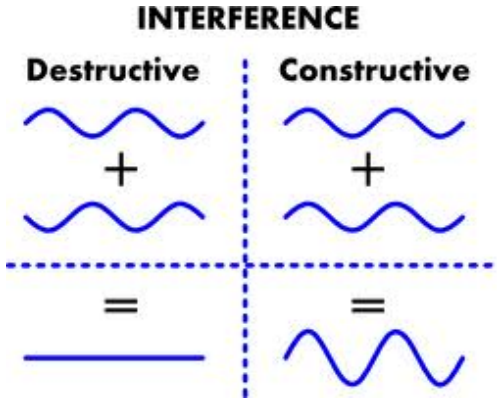


- Quantum computation = superposition + interference

1. Start with qubits in some simple state (e.g. all $|0\rangle$)

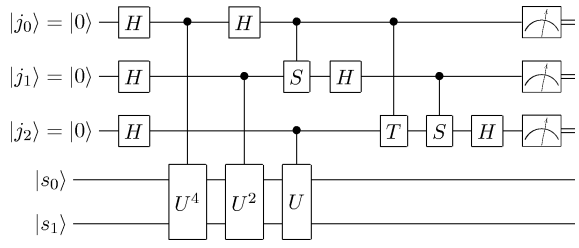
Quantum computers in a nutshell

- Waves can strengthen or weaken each other:



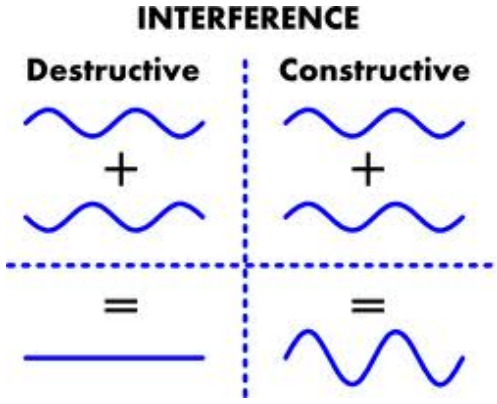
- Quantum computation = superposition + interference

1. Start with qubits in some simple state (e.g. all $|0\rangle$)
2. Run circuit of "elementary gates" creating the right interference, so the final state has most of its weight on solutions to your problem



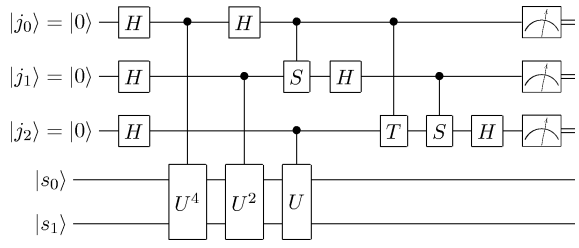
Quantum computers in a nutshell

- Waves can strengthen or weaken each other:



- Quantum computation = superposition + interference

1. Start with qubits in some simple state (e.g. all $|0\rangle$)
2. Run circuit of "elementary gates" creating the right interference, so the final state has most of its weight on solutions to your problem



3. Measuring the final state then gives solution

Where do we stand today?

Where do we stand today?

- We are entering the NISQ era (Preskill'18):
  Noisy Intermediate-Scale Quantum technology

Where do we stand today?

- We are entering the NISQ era (Preskill'18):
  Noisy Intermediate-Scale Quantum technology
- IBM, Google, Intel are close to 50-70 reasonably good qubits.

Where do we stand today?

- We are entering the NISQ era (Preskill'18):
  Noisy Intermediate-Scale Quantum technology
- IBM, Google, Intel are close to 50-70 reasonably good qubits.

  But 50-70 qubits is not a lot: classical computers have billions of bits

Where do we stand today?

- We are entering the NISQ era (Preskill'18):
  Noisy Intermediate-Scale Quantum technology
- IBM, Google, Intel are close to 50-70 reasonably good qubits.

  But 50-70 qubits is not a lot: classical computers have billions of bits. And "reasonably good" is also not great

Where do we stand today?

- We are entering the NISQ era (Preskill'18):
  Noisy Intermediate-Scale Quantum technology
- IBM, Google, Intel are close to 50-70 reasonably good qubits.

  But 50-70 qubits is not a lot: classical computers have billions of bits. And "reasonably good" is also not great
- We'll need error-correction to deal with errors,
  and that will require many more physical qubits

Where do we stand today?

- We are entering the NISQ era (Preskill'18):
  Noisy Intermediate-Scale Quantum technology
- IBM, Google, Intel are close to 50-70 reasonably good qubits.

  But 50-70 qubits is not a lot: classical computers have billions of bits. And "reasonably good" is also not great
- We'll need error-correction to deal with errors,
  and that will require many more physical qubits
- "Quantum supremacy" may be reached soon:
  some quantum computation that cannot be simulated on today's best supercomputers in a reasonable amount of time

Where do we stand today?

- We are entering the NISQ era (Preskill'18):
  Noisy Intermediate-Scale Quantum technology
- IBM, Google, Intel are close to 50-70 reasonably good qubits.

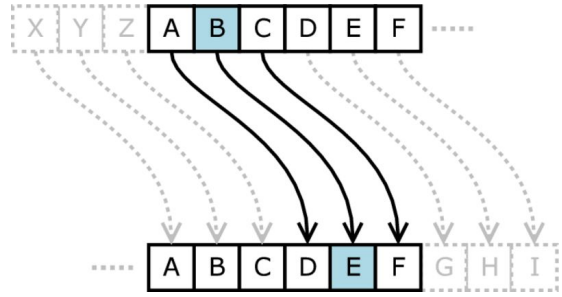
  But 50-70 qubits is not a lot: classical computers have billions of bits. And "reasonably good" is also not great
- We'll need error-correction to deal with errors,
  and that will require many more physical qubits
- "Quantum supremacy" may be reached soon:
  some quantum computation that cannot be simulated on today's best supercomputers in a reasonable amount of time
- But useful quantum supremacy is still years away

Potential impact area 1: cryptography

- The ancient art of secret communication

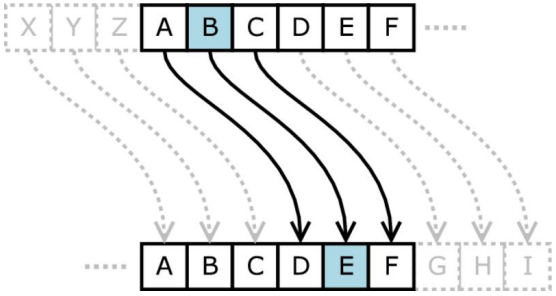
Potential impact area 1: cryptography

- The ancient art of secret communication
- Julius Caesar encrypted his letters
  by shifting the alphabet (easy to break)



Potential impact area 1: cryptography

- The ancient art of secret communication

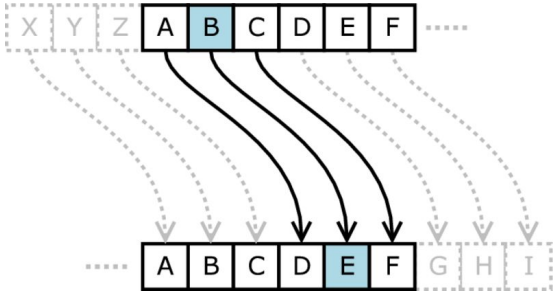


- Julius Caesar encrypted his letters by shifting the alphabet (easy to break)

- The nazis encrypted their messages using fancy "Enigma" machines with secret settings that changed every day (broken by Turing and others using the first computers)

Potential impact area 1: cryptography

- The ancient art of secret communication



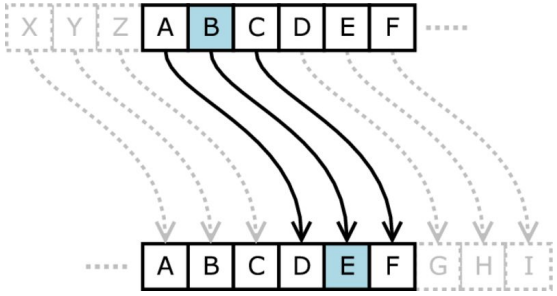
- Julius Caesar encrypted his letters by shifting the alphabet (easy to break)

- The nazis encrypted their messages using fancy "Enigma" machines with secret settings that changed every day (broken by Turing and others using the first computers)

- Since the 1970s: more systematic, mathematical study

Potential impact area 1: cryptography

- The ancient art of secret communication



- Julius Caesar encrypted his letters by shifting the alphabet (easy to break)

- The nazis encrypted their messages using fancy "Enigma" machines with secret settings that changed every day (broken by Turing and others using the first computers)

- Since the 1970s: more systematic, mathematical study
- Two branches: codemakers and codebreakers

Codebreaking

Codebreaking

- Public-key cryptosystems are great

Codebreaking

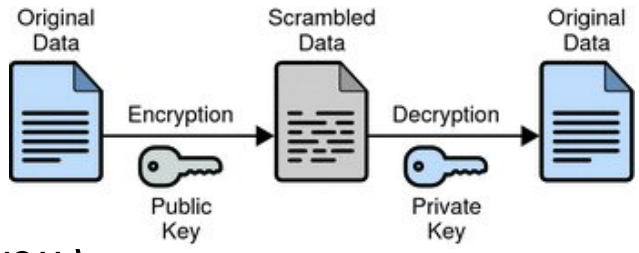
- Public-key cryptosystems are great:
  - you choose private key and public key

Codebreaking

- Public-key cryptosystems are great:
  - you choose private key and public key
  - everybody with the public key
    can send you encrypted messages

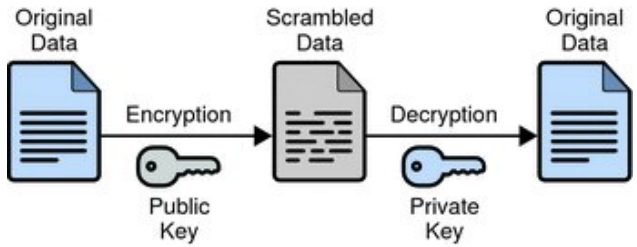
Codebreaking

- Public-key cryptosystems are great:
  - you choose private key and public key
  - everybody with the public key can send you encrypted messages
  - messages can only be decrypted by someone with the private key (=only you)



Codebreaking

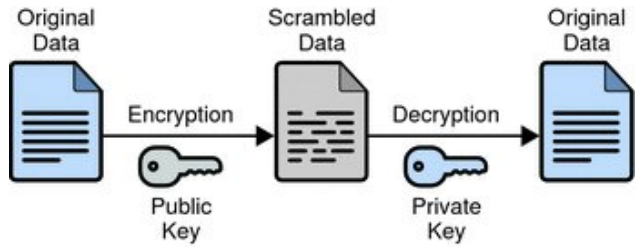
- Public-key cryptosystems are great:
  - you choose private key and public key
  - everybody with the public key can send you encrypted messages
  - messages can only be decrypted by someone with the private key (=only you)



. . . unless they can solve some hard math problem

Codebreaking

- Public-key cryptosystems are great:
  - you choose private key and public key
  - everybody with the public key can send you encrypted messages
  - messages can only be decrypted by someone with the private key (=only you)



. . . unless they can solve some hard math problem

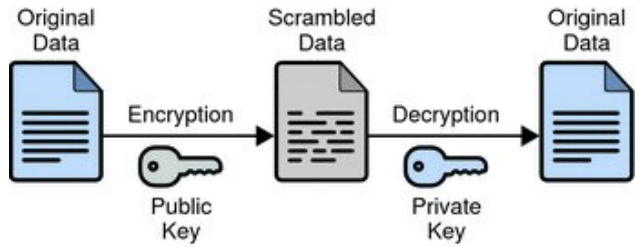
- Most public-key crypto is based on the assumed hardness of

  - factoring large integers (RSA), or

  - finding discrete logarithms (Diffie-Hellman, Elliptic curve)

Codebreaking

- Public-key cryptosystems are great:
  - you choose private key and public key
  - everybody with the public key can send you encrypted messages
  - messages can only be decrypted by someone with the private key (=only you)



  . . . unless they can solve some hard math problem

- Most public-key crypto is based on the assumed hardness of

  - factoring large integers (RSA), or

  - finding discrete logarithms (Diffie-Hellman, Elliptic curve)

- Shor's algorithm breaks this using a few thousand good qubits

Is this an imminent threat?

Is this an imminent threat?

- Relax, quantum computers ain't gonna happen anytime soon...

Is this an imminent threat?

- Relax, quantum computers ain't gonna happen anytime soon...
- Maybe, maybe not.

Is this an imminent threat?

- Relax, quantum computers
  ain't gonna happen anytime soon...

- Maybe, maybe not.

  But many countries have laws requiring top-secret documents to be protected for the next 20-30 years.

Is this an imminent threat?

- Relax, quantum computers
  ain't gonna happen anytime soon...

- Maybe, maybe not.

  But many countries have laws requiring top-secret documents to be protected for the next 20-30 years.

  If somebody steals your encrypted records now and decrypts it 10 years later using a quantum computer, that's still bad.

Is this an imminent threat?

- Relax, quantum computers
  ain't gonna happen anytime soon...

- Maybe, maybe not.

  But many countries have laws requiring top-secret documents to be protected for the next 20-30 years.

  If somebody steals your encrypted records now and decrypts it 10 years later using a quantum computer, that's still bad.

- Also, changing our crypto infrastructure will take a long time

Is this an imminent threat?

- Relax, quantum computers
  ain't gonna happen anytime soon...

- Maybe, maybe not.

  But many countries have laws requiring top-secret documents to be protected for the next 20-30 years.

  If somebody steals your encrypted records now and decrypts it 10 years later using a quantum computer, that's still bad.

- Also, changing our crypto infrastructure will take a long time

- So, how to fix
  cryptography
  against quantum
  adversaries?

Is this an imminent threat?

- Relax, quantum computers ain't gonna happen anytime soon...

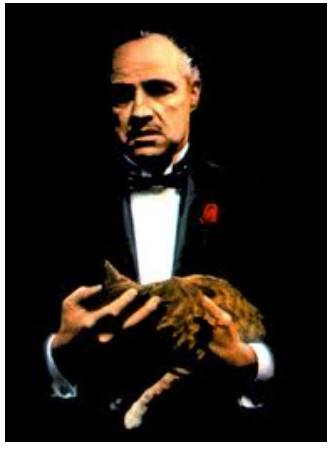
- Maybe, maybe not.

  But many countries have laws requiring top-secret documents to be protected for the next 20-30 years.

  If somebody steals your encrypted records now and decrypts it 10 years later using a quantum computer, that's still bad.

- Also, changing our crypto infrastructure will take a long time

- So, how to fix cryptography against quantum adversaries?



Is this an imminent threat?

- Relax, quantum computers ain't gonna happen anytime soon...

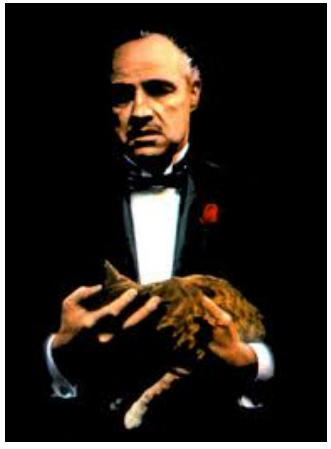
- Maybe, maybe not.

  But many countries have laws requiring top-secret documents to be protected for the next 20-30 years.

  If somebody steals your encrypted records now and decrypts it 10 years later using a quantum computer, that's still bad.

- Also, changing our crypto infrastructure will take a long time

- So, how to fix cryptography against quantum adversaries?



Is this an imminent threat?

- Relax, quantum computers ain't gonna happen anytime soon...

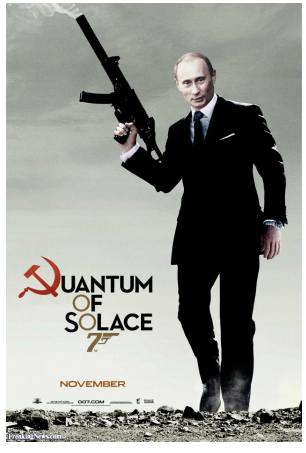
- Maybe, maybe not.

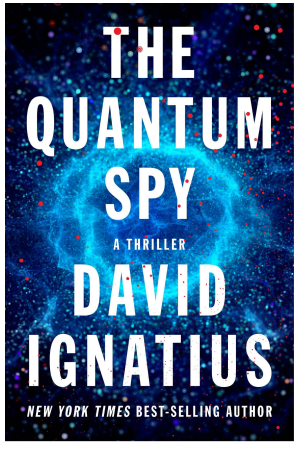
  But many countries have laws requiring top-secret documents to be protected for the next 20-30 years.

  If somebody steals your encrypted records now and decrypts it 10 years later using a quantum computer, that's still bad.

- Also, changing our crypto infrastructure will take a long time

- So, how to fix cryptography against quantum adversaries?





Classical codemaking: post-quantum cryptography

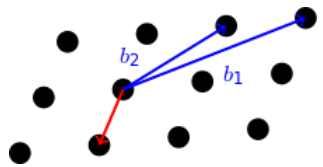
Classical codemaking: post-quantum cryptography

- Minimal adaptation: keep the idea of public-key crypto, but base it on other math problems than factoring or discrete log.

Classical codemaking: post-quantum cryptography

- Minimal adaptation: keep the idea of public-key crypto, but base it on other math problems than factoring or discrete log.

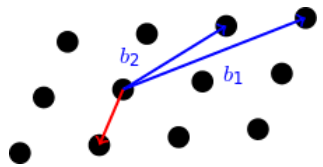
  Prominent examples: lattice problems, error-correcting code problems, ...



Classical codemaking: post-quantum cryptography

- Minimal adaptation: keep the idea of public-key crypto, but base it on other math problems than factoring or discrete log.

  Prominent examples: lattice problems, error-correcting code problems, ...

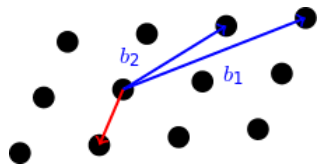


- Advantages: Users only need classical computers, we can keep our efficient public-key infrastructure

Classical codemaking: post-quantum cryptography

- Minimal adaptation: keep the idea of public-key crypto, but base it on other math problems than factoring or discrete log.

  Prominent examples: lattice problems, error-correcting code problems, ...



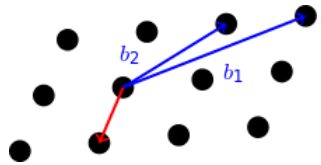
- Advantages: Users only need classical computers, we can keep our efficient public-key infrastructure

- Disadvantages: Are these systems secure against quantum computers?

Classical codemaking: post-quantum cryptography

- Minimal adaptation: keep the idea of public-key crypto, but base it on other math problems than factoring or discrete log.

  Prominent examples: lattice problems, error-correcting code problems, ...



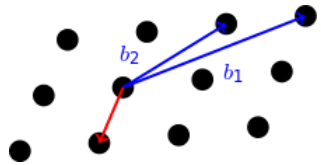
- Advantages: Users only need classical computers, we can keep our efficient public-key infrastructure

- Disadvantages: Are these systems secure against quantum computers? Who knows; not enough research yet

Classical codemaking: post-quantum cryptography

- Minimal adaptation: keep the idea of public-key crypto, but base it on other math problems than factoring or discrete log.

  Prominent examples: lattice problems, error-correcting code problems, ...



- Advantages: Users only need classical computers, we can keep our efficient public-key infrastructure

- Disadvantages: Are these systems secure against quantum computers? Who knows; not enough research yet

- NIST is running a competition for the best candidate scheme

Quantum codemaking: quantum cryptography

Quantum codemaking: quantum cryptography

- Use quantum to induce an information-gain-vs-disturbance tradeoff: if adversary learns a lot about state of quantum channel, then they necessarily disturb it, and will be detected

Quantum codemaking: quantum cryptography

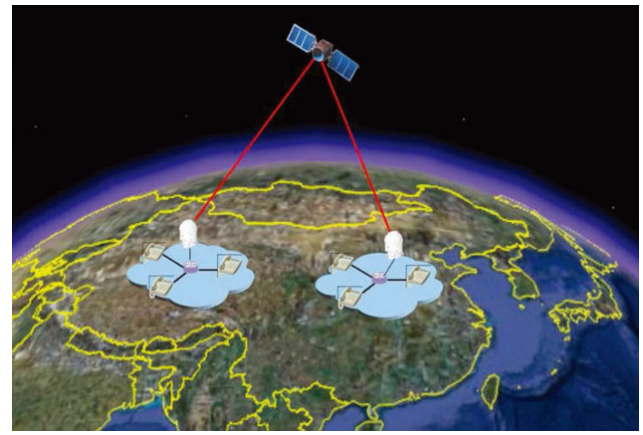
- Use quantum to induce an information-gain-vs-disturbance tradeoff: if adversary learns a lot about state of quantum channel, then they necessarily disturb it, and will be detected
- BB'84 quantum key distribution: Alice and Bob can obtain a shared secret key by communicating over a *public* quantum channel and a *public authenticated* classical channel

Quantum codemaking: quantum cryptography

- Use quantum to induce an information-gain-vs-disturbance tradeoff: if adversary learns a lot about state of quantum channel, then they necessarily disturb it, and will be detected
- BB'84 quantum key distribution: Alice and Bob can obtain a shared secret key by communicating over a *public* quantum channel and a *public authenticated* classical channel
- Advantages: Information-theoretic security against quantum adversary

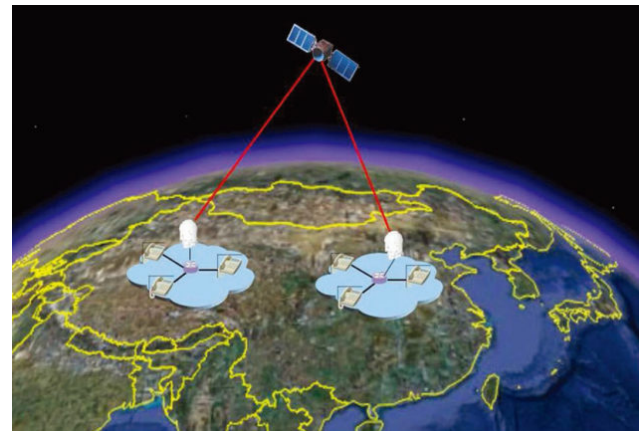
Quantum codemaking: quantum cryptography

- Use quantum to induce an information-gain-vs-disturbance tradeoff: if adversary learns a lot about state of quantum channel, then they necessarily disturb it, and will be detected
- BB'84 quantum key distribution: Alice and Bob can obtain a shared secret key by communicating over a *public* quantum channel and a *public authenticated* classical channel
- Advantages: Information-theoretic security against quantum adversary. Doable with current technology, even via satellites!



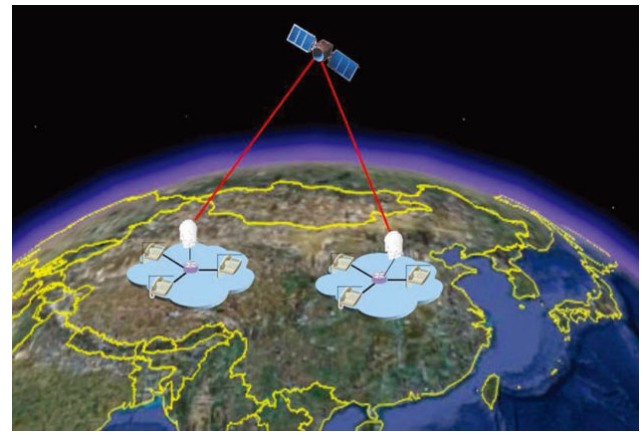
Quantum codemaking: quantum cryptography

- Use quantum to induce an information-gain-vs-disturbance tradeoff: if adversary learns a lot about state of quantum channel, then they necessarily disturb it, and will be detected
- BB'84 quantum key distribution: Alice and Bob can obtain a shared secret key by communicating over a *public* quantum channel and a *public authenticated* classical channel
- Advantages: Information-theoretic security against quantum adversary. Doable with current technology, even via satellites!
- Disadvantages: Inefficient point-to-point communication.



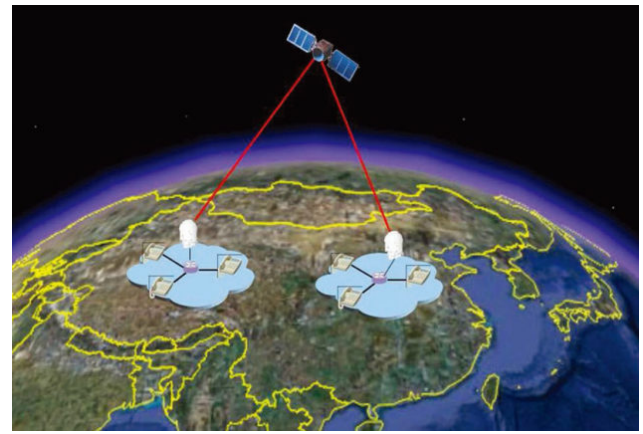
Quantum codemaking: quantum cryptography

- Use quantum to induce an information-gain-vs-disturbance tradeoff: if adversary learns a lot about state of quantum channel, then they necessarily disturb it, and will be detected
- BB'84 quantum key distribution: Alice and Bob can obtain a shared secret key by communicating over a *public* quantum channel and a *public authenticated* classical channel
- Advantages: Information-theoretic security against quantum adversary. Doable with current technology, even via satellites!
- Disadvantages: Inefficient point-to-point communication. Limited distance.



Quantum codemaking: quantum cryptography

- Use quantum to induce an information-gain-vs-disturbance tradeoff: if adversary learns a lot about state of quantum channel, then they necessarily disturb it, and will be detected
- BB'84 quantum key distribution: Alice and Bob can obtain a shared secret key by communicating over a *public* quantum channel and a *public authenticated* classical channel
- Advantages: Information-theoretic security against quantum adversary. Doable with current technology, even via satellites!
- Disadvantages: Inefficient point-to-point communication. Limited distance. Current implementations have often been hacked



Potential impact area 2: optimization

Potential impact area 2: optimization

- Optimization is one of the main applications of computers in the real world: allocating resources to jobs, scheduling lectures, optimizing designs, minimizing energy use, etc.

Potential impact area 2: optimization

- Optimization is one of the main applications of computers in the real world: allocating resources to jobs, scheduling lectures, optimizing designs, minimizing energy use, etc.
- Quantum computers can help

Potential impact area 2: optimization

- Optimization is one of the main applications of computers in the real world: allocating resources to jobs, scheduling lectures, optimizing designs, minimizing energy use, etc.
- Quantum computers can help:
  - Grover's search algorithm

Potential impact area 2: optimization

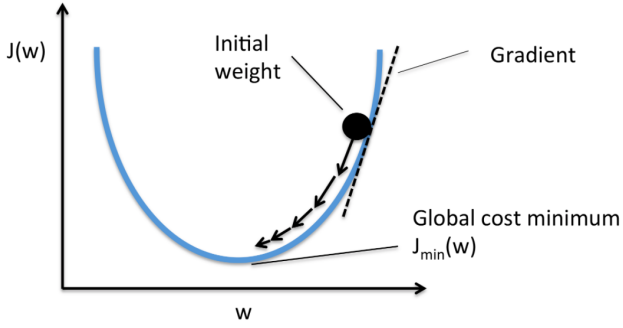
- Optimization is one of the main applications of computers in the real world: allocating resources to jobs, scheduling lectures, optimizing designs, minimizing energy use, etc.
- Quantum computers can help:
  - Grover's search algorithm
  - Finding the shortest path on a map

Potential impact area 2: optimization

- Optimization is one of the main applications of computers in the real world: allocating resources to jobs, scheduling lectures, optimizing designs, minimizing energy use, etc.
- Quantum computers can help:
  - Grover's search algorithm
  - Finding the shortest path on a map
  - Speed-ups for linear programs

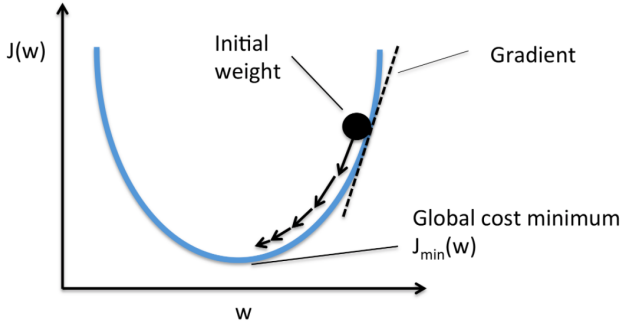
Potential impact area 2: optimization

- Optimization is one of the main applications of computers in the real world: allocating resources to jobs, scheduling lectures, optimizing designs, minimizing energy use, etc.
- Quantum computers can help:
  - Grover's search algorithm
  - Finding the shortest path on a map
  - Speed-ups for linear programs
  - Gradient descent towards minimum



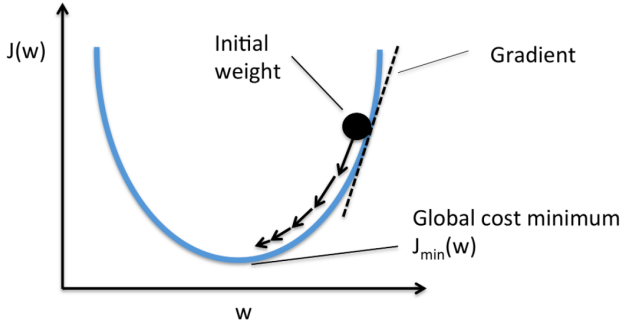
Potential impact area 2: optimization

- Optimization is one of the main applications of computers in the real world: allocating resources to jobs, scheduling lectures, optimizing designs, minimizing energy use, etc.
- Quantum computers can help:
  - Grover's search algorithm
  - Finding the shortest path on a map
  - Speed-ups for linear programs
  - Gradient descent towards minimum
  - Finite-element methods



Potential impact area 2: optimization

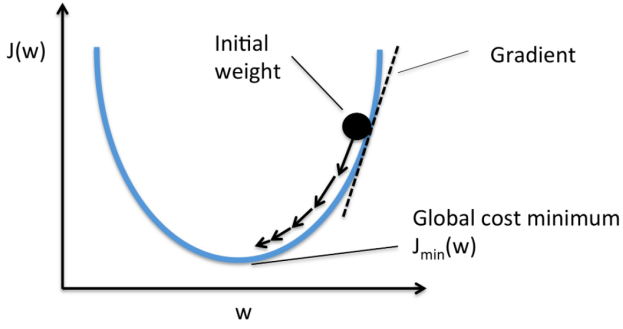
- Optimization is one of the main applications of computers in the real world: allocating resources to jobs, scheduling lectures, optimizing designs, minimizing energy use, etc.
- Quantum computers can help:
  - Grover's search algorithm
  - Finding the shortest path on a map
  - Speed-ups for linear programs
  - Gradient descent towards minimum
  - Finite-element methods



- Typically these only give limited ("polynomial") speed-up; whether that's worthwhile depends on the cost of a QC

Potential impact area 2: optimization

- Optimization is one of the main applications of computers in the real world: allocating resources to jobs, scheduling lectures, optimizing designs, minimizing energy use, etc.
- Quantum computers can help:
  - Grover's search algorithm
  - Finding the shortest path on a map
  - Speed-ups for linear programs
  - Gradient descent towards minimum
  - Finite-element methods



- Typically these only give limited ("polynomial") speed-up; whether that's worthwhile depends on the cost of a QC
- Classical input needs to be accessible in superposition, so needs to be stored in Quantum Random Access Memory

Quantum machine learning

Quantum machine learning

- Machine learning has gotten hugely successful in the last 5 years

Quantum machine learning

- Machine learning has gotten hugely successful in the last 5 years

- After choosing set $\mathcal{M}$ of possible models & cleaning up data

Quantum machine learning

- Machine learning has gotten hugely successful in the last 5 years

- After choosing set $\mathcal{M}$ of possible models & cleaning up data, machine learning boils down to an optimization problem:

$$\max_{m \in \mathcal{M}} \text{ fit of } m \text{ with the data}$$

Quantum machine learning

- Machine learning has gotten hugely successful in the last 5 years

- After choosing set $\mathcal{M}$ of possible models & cleaning up data, machine learning boils down to an optimization problem:

  $$\max_{m \in \mathcal{M}} \text{ fit of } m \text{ with the data}$$

  Quantum computers can speed this up (in some cases)

Quantum machine learning

- Machine learning has gotten hugely successful in the last 5 years

- After choosing set $\mathcal{M}$ of possible models & cleaning up data, machine learning boils down to an optimization problem:

  $$\max_{m \in \mathcal{M}} \text{ fit of } m \text{ with the data}$$

  Quantum computers can speed this up (in some cases)

- Often the data consists of vectors in some large dimension d. Can try to prepare those as $\log_2(d)$-qubit states, manipulate those with quantum algorithms

Quantum machine learning

- Machine learning has gotten hugely successful in the last 5 years

- After choosing set $\mathcal{M}$ of possible models & cleaning up data, machine learning boils down to an optimization problem:

  $$\max_{m \in \mathcal{M}} \text{ fit of } m \text{ with the data}$$

  Quantum computers can speed this up (in some cases)

- Often the data consists of vectors in some large dimension d. Can try to prepare those as $\log_2(d)$-qubit states, manipulate those with quantum algorithms. Easier said than done...

Potential impact area 3: simulation

Potential impact area 3: simulation

- Much effort on understanding quantum systems for materials, batteries, drugs, high-temperature superconductivity etc.

Potential impact area 3: simulation

- Much effort on understanding quantum systems for materials, batteries, drugs, high-temperature superconductivity etc.

Potential impact area 3: simulation

- Much effort on understanding quantum systems for materials, batteries, drugs, high-temperature superconductivity etc.
- Sophisticated classical methods hit a wall for larger systems, because of the exponential number of amplitudes in a state

Potential impact area 3: simulation

- Much effort on understanding quantum systems for materials, batteries, drugs, high-temperature superconductivity etc.
- Sophisticated classical methods hit a wall for larger systems, because of the exponential number of amplitudes in a state
- Think of quantum computer as universal quantum simulator: given a sufficiently simple description of a physical system ("Hamiltonian"), a quantum computer can simulate the evolution of a given initial state for some time t

Potential impact area 3: simulation

- Much effort on understanding quantum systems for materials, batteries, drugs, high-temperature superconductivity etc.
- Sophisticated classical methods hit a wall for larger systems, because of the exponential number of amplitudes in a state
- Think of quantum computer as universal quantum simulator: given a sufficiently simple description of a physical system ("Hamiltonian"), a quantum computer can simulate the evolution of a given initial state for some time t
- This could lead to better materials, drugs, ...

Potential impact area 3: simulation

- Much effort on understanding quantum systems for materials, batteries, drugs, high-temperature superconductivity etc.
- Sophisticated classical methods hit a wall for larger systems, because of the exponential number of amplitudes in a state
- Think of quantum computer as universal quantum simulator: given a sufficiently simple description of a physical system ("Hamiltonian"), a quantum computer can simulate the evolution of a given initial state for some time t
- This could lead to better materials, drugs, ...
- Could already be useful with 100s good qubits (unlike Shor)

Conclusion

- Quantum mechanics: best physical theory we have

Conclusion

- Quantum mechanics: best physical theory we have
- Fundamentally different from classical physics: superposition, interference, entanglement

Conclusion

- Quantum mechanics: best physical theory we have
- Fundamentally different from classical physics: superposition, interference, entanglement
- Quantum computers can use these non-classical effects for many useful things: cryptography, optimization, simulation.

  Though it will probably remain a "special purpose" computer

Conclusion

- Quantum mechanics: best physical theory we have
- Fundamentally different from classical physics: superposition, interference, entanglement
- Quantum computers can use these non-classical effects for many useful things: cryptography, optimization, simulation.

  Though it will probably remain a "special purpose" computer
- People are working hard on physical implementations

Conclusion

- Quantum mechanics: best physical theory we have
- Fundamentally different from classical physics: superposition, interference, entanglement
- Quantum computers can use these non-classical effects for many useful things: cryptography, optimization, simulation.

  Though it will probably remain a "special purpose" computer
- People are working hard on physical implementations
- What will this mean in practice?

  We'll see. . . though we are still far from a large-scale quantum computer