Fundamental Concepts

"The big picture"

Definition:

Quantum computation (QC)
Quantum information theory (QIT)

"The study of the information processing tasks that can be accomplished using quantum mechanical systems"

Beginning of C20

A crisis in physics:

absurd predictions??

early 1920s - quantum mechanics

... applied to

structure of atom,
nuclear fusion,
superconductors,
structure of DNA
elementary particles

Quantum Mechanics ??

A mathematical framework for the construction of physical theories.

Simple rules but counter-intuitive

Critics ?

Einstein

Early result in QC/QIT:

No-Cloning Theorem (early 1980s)

YES

NO!!

Cloning of quantum information
implies
faster-than-light signalling

} NOT POSSIBLE

Since 1970s,

Control over single quantum systems possible

... e.g. ...

atom trap

scanning tunneling microscope

electronic devices

State-of-the-art:

quantum computers: dozens of operations on a few quantum bits

prototypes for quantum key distribution: working and "nearly" useful

The future?: Large-scale quantum information processing?

Another Discipline - Computer Science

Alan Turing (1936):

Universal Turing Machine

Simulates

any other Turing machine

Church-Turing thesis

Any algorithm on arbitrary hardware can be performed on a universal Turing machine.

Moore's Law

Computer power doubles once every two years

.... size limit ??

.... quantum effects ??

.... move to a different computing paradigm?

A classical computer can simulate a quantum computer but ...

it appears that ...

a classical computer cannot efficiently simulate a quantum computer.

QCs offer a potential speed advantage over classical computers

Efficient / Inefficient?

Computational Complexity:

An efficient algorithm runs in time polynomial in problem size. An inefficient algorithm requires superpolynomial (typically exponential) size.

Strong Church-Turing Thesis

Any algorithmic process can be simulated efficiently using a Turing machine,

So,

a standard Turing machine may efficiently simulate any machine we use.

Challenges to Strong Church-Turing Thesis

Analog Computers:

Appear to efficiently solve problems having no efficient solution on a Turing machine.

.... but when realistic noise assumptions taken into account, advantage disappears.

Quantum Computers:

Appear to efficiently solve problems having no efficient solution on a Turing machine.

... noise problem tackled by quantum error-correcting codes and fault-tolerant QC.

Solovay-Strassen Test

Efficient randomised algorithm to test for integer primality

outputs ⟶ probably prime
or
definitely composite

repeated testing ⟶ prime with near-certainty
or
composite

..... tweaked Strong Church-Turing thesis ?

Any algorithmic process can be simulated efficiently using a probabilistic Turing machine

David Deutsch (1985)

used laws of physics to derive an even stronger version of the Church-Turing thesis.

.... define a computational device capable of efficiently simulating an arbitrary physical system.

$\Rightarrow$ must be based on principles of quantum mechanics.

Universal Quantum Computer – Deutsch

Open Problem: Can the UQC efficiently simulate an arbitrary physical system?

....

are there more powerful models?

... e.g. beyond quantum mechanics?

Deutsch asked:

Can a QC efficiently solve problems with no efficient solution using a probabilistic Turing machine?

He constructed a simple example suggesting precisely this.

Peter Shor (1994)

Factoring
Discrete Log
} - Can be solved efficiently on a QC!!

Lov Grover (1995)

Unstructured Search - Can be solved significantly faster on a QC.

Feynman (1982)

Suggested building computers using principles of quantum mechanics,

so as to ...

simulate quantum mechanical systems

... future application for QCs...

.. simulate physical systems too difficult to simulate on a classical computer....

What other problems can be solved faster on a QC than a classical computer??

... er....

... um.... ...um...

.... er....

..... um ..... ?!

Pessimist's View : QCs are useless
and/or unrealisable

Optimist's View : Be patient ..... algorithms are
hard...
...complexity classes?...

My View: The mathematics is globally useful...
... classical/quantum hybrids are the
way to go....

Shannon (1948)

Defined information mathematically.

Two questions:

1. Resources required to send information over a communications channel?
2. Can transmitted information be protected against channel noise?

Noiseless Channel Coding Theorem (Shannon)

Quantifies physical resources required to store the output from an information source.

Noisy Channel Coding Theorem (Shannon)

Quantifies and limits the amount of information that can be reliably transmitted through a noisy channel.

... Solution ... error-correcting codes

... many practically useful near-Shannon limit codes now exist.

Schumacher (1995)

Noiseless coding theorem for....

.....quantum information.....

... defined quantum bit (qubit) as a resource

... but we do not yet have a noisy channel coding theorem for quantum information...

...but quantum error-correction allows for effective computation and communication over noisy physical systems.

Steane, Calderbank, Shor (1998)

CSS Codes

... subsumed by

Calderbank, Rains, Shor, Sloane, Gottesman

Stabilizer codes

(including GF(4)-additive codes
and graph codes)

Transmission of classical information on a quantum channel?

Bennett, Wiesner (1992) - Superdense Coding

Transmit two classical bits, while only transmitting one quantum bit.

Distributed Quantum Computation

QCs require exponentially less communication to solve certain problems than would be required if the networked computers were classical.

..... QIT networks?

... quantum network coding? (2005, 2006)

.... LDPC on hybrid quantum/classical graphs?
(2007, Bergen?)

What is the information carrying capability of a network of quantum channels? ...many open problems.

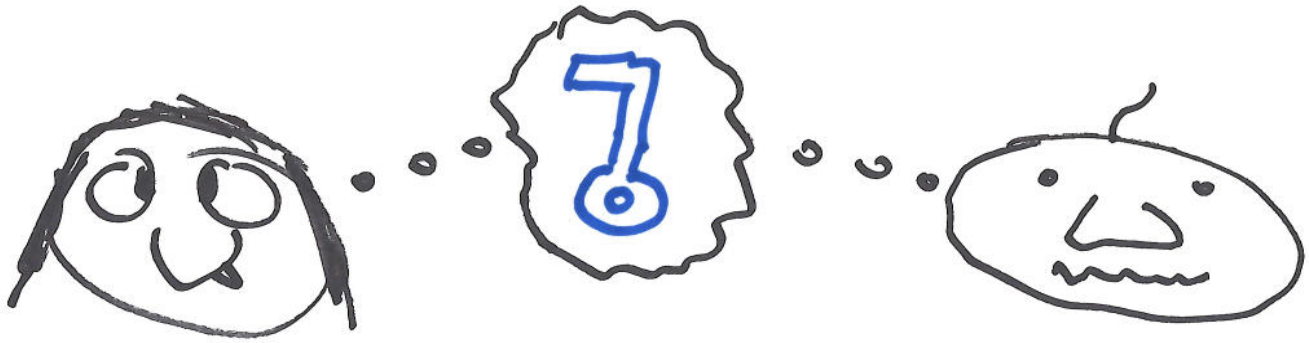
Cryptography

Private Key Systems

Public Key Systems

Private-Key

Alice - Bob share private key



Problem: Key distribution

Solution: QKD - Quantum Key Distribution

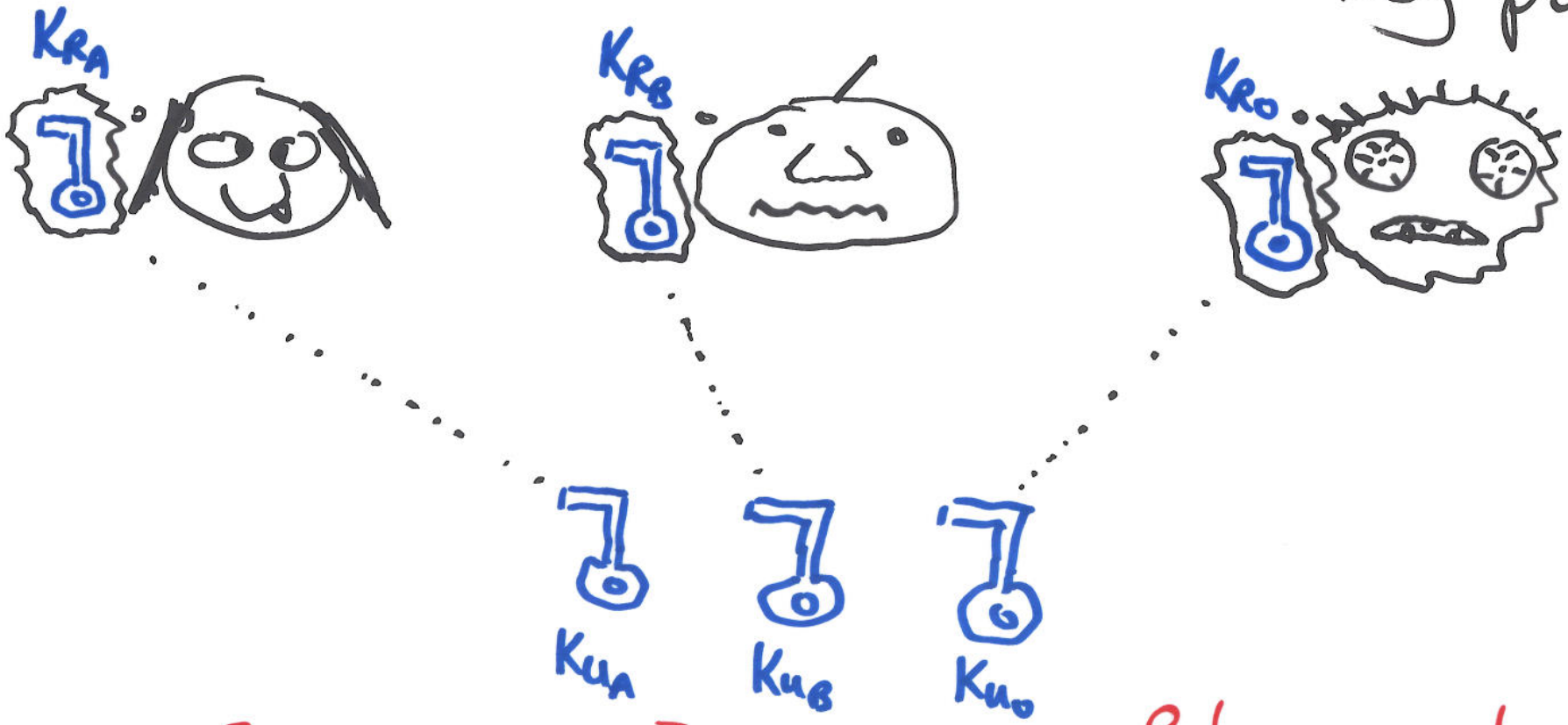
Wiesner (1960s ... publication rejected)

Bennett, Brassard (1984), BB84 protocol

... observation disturbs system. If key transmission observed, then disturbance flagged - start again.

Public-Key (1960s/70s)

Alice-Bob-Odd each have a public/private key pair



$[Alice \xrightarrow{M} Bob]_{K_{UB}}$:

Bob can read message using K_{RB}.
Odd cannot read message.

QKD is now operational.

"Unconditional" security.

"Useful" physical realisations exist.

Is it worth the expense?

Note: QKD solves the problem of classical key distribution.

Unlike private-key systems,
public-key system does not require
pre-shared secret key.

RSA implements public-key using factoring.

"Broken" by QC (Shor 1994)

Quantum Entanglement

A quantum resource.

... entanglement can be shared, used, ...

.... large entanglement means that the system is strongly non-classical.

.... many measures

The Future

Physical view of computation/information.

Information-theoretic view of physical systems.

Computational-theoretic view of physical systems.