Quantum Computing & Cryptography

Steve Vickers

Non-examinable introduction
- Quantum key distribution
  - already in use, with polarized photons
  - quantum physics \(\Rightarrow\) no passive eavesdropping
- Quantum computers
  - no practical ones yet
  - quantum physics \(\Rightarrow\) clever probabilistic algorithms
  - no efficient classical simulation
  - Shor's factorization algorithm would break RSA

Light as waves
= vibrations in electromagnetic field
transverse to direction of travel
180° of possible vibration directions

Most light is mixture of all directions

Polarized light - only oscillates in some directions

Vertically polarized
\(\uparrow\)

Also: diagonally polarized \(\uparrow\ \& \ \downarrow\) etc.

Also: circularly polarized - direction rotates

Polarizing filter
- passes light vibrating one direction
- stops it for other direction

\(\uparrow\) polarized light

Unpolarized light

Second filter at 90° will stop light altogether
**Application**

Polarizing sunglasses

- Sunblind blocks direct rays
- What about glare (reflected rays)?

- Low sun
- Wet road

**Interesting phenomenon**

Vertically polarized light

- Filter in various orientations
- All light passes
- All light blocked
- 50% of light passes
- And it comes through diagonally polarized

**Another application**

3D cinema

- Want left & right eyes to see slightly different pictures => illusion of depth
- Two pictures mixed together, with opposite circular polarizations
- Wear glasses with circular polarizing filters

- Why circular?
Birefringent crystals
refract in two different ways
input splits into two polarized beams

For birefringence:

Explanation (Einstein)
- Light comes in particles (photons)
- Energy of each photon depends on frequency
  - Need photons of at least a certain energy to dislodge electrons & make electricity

<table>
<thead>
<tr>
<th>Low frequency energy</th>
<th>High frequency energy</th>
</tr>
</thead>
<tbody>
<tr>
<td>microwaves</td>
<td>X-rays</td>
</tr>
<tr>
<td>radio</td>
<td>visible light</td>
</tr>
<tr>
<td>infra-red (radiant heat)</td>
<td>ultra-violet</td>
</tr>
</tbody>
</table>

Photons Light comes in particles (quanta)
How do we know?
e.g. photocells
Light in electricity out
Input light must be at least a certain frequency — or no electricity out (no matter how bright light is)
Weird
Photons still behave like waves
e.g. polarization
each photon has its own polarization state

Also e.g. diffraction
Waves can form interference patterns
A photon can interfere with itself - probabilistic behaviour
constructive) interference = \{high\} probability
destructive) interference = \{low\} probability

Measurement
To find a photon's polarization state
you measure it
- e.g. pass it through birefringent crystal,
  see where it comes out
BUT each orientation of crystal measures
only two polarization states
e.g. \[ \text{for } \uparrow \leftrightarrow \uparrow \]
measurement for \[ \uparrow \leftrightarrow \downarrow \] or \[ \uparrow \leftrightarrow \ \text{left-right} \]

Single polarized photon & birefringent crystal

\[ \text{\$\$ photon has same polarization as before and you know which it is} \]
\[ \text{\$\$ photon is randomly reduced to } \uparrow \text{ or } \leftrightarrow \text{. You know which, but you know nothing about original direction} \]

Range of polarization states - lie on sphere

Other points correspond to other polarization orientations
Infinitely many possible states, but...
to measure you must choose an axis & accept one of only two possible results
\[ \text{:: like a bit - 2 bit} \]
**Preparation**

Also to prepare a photon in a known state: measure it!

Result says what its state is now.

If it comes out here: you’ve prepared a photon in state $\uparrow$.

Here: photon in state $\leftrightarrow$.

Not quite as simple as this, but it can be done.

**Quantum key distribution**

BB 84 = Bennett & Brassard 1984

- Use polarized photons to share a private key
- Any eavesdropping disturbs polarization in a way that can be detected
- Technology already exists
  - generate single photons
  - manipulate their polarizations
  - transmit - fibre optics or open air

**Protocol**

$\uparrow, \downarrow$ encode 0

$\leftrightarrow$ encode 1

- Alice prepares a string of photons
  - chooses $\uparrow$ or $\downarrow$ at random to prepare each one
  - sends them all to Bob
- Bob measures each for (at random) $\uparrow$ or $\downarrow$
- They tell each other what preparation/measurement types they used for each photon
- Where types disagree, photon is wasted
- Where they agree, a bit has been communicated securely

**e.g.**

<table>
<thead>
<tr>
<th>Alice prepares</th>
<th>Bob measures</th>
<th>bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>state</td>
<td>type</td>
<td>type</td>
</tr>
<tr>
<td>$\uparrow$</td>
<td>$\leftrightarrow$</td>
<td>$\leftrightarrow$</td>
</tr>
<tr>
<td>$\uparrow$</td>
<td>$\leftrightarrow$</td>
<td>$\leftrightarrow$</td>
</tr>
<tr>
<td>$\uparrow$</td>
<td>$\leftrightarrow$</td>
<td>$\leftrightarrow$</td>
</tr>
<tr>
<td>$\uparrow$</td>
<td>$\leftrightarrow$</td>
<td>$\leftrightarrow$</td>
</tr>
</tbody>
</table>

Shared insecurely

Good bits = secure key = 001
Eavesdroppers

- Eve cannot measure photons and send them on to Bob unchanged.
- To measure them, she must guess whether Alice used $\uparrow$ or $\downarrow$.
- Wrong guess $\Rightarrow$ messes up the polarization state.
- Alice and Bob can detect this statistically if they tell each other the states of some test photons as well as the types. **Those photons won't be available for the key.**

Test photons

Alice, Bob tell each other types and results.

- e.g. Alice prepares $\uparrow$, Bob measures type $\downarrow$.
- Bob should always get the same result $\uparrow$.
- Eve guesses type:
  - 50% $\Rightarrow$ she always gets result $\uparrow$.
  - 50% $\Rightarrow$ she gets result $\uparrow$ or $\downarrow$ at random.
  - Retransmits $\uparrow$ to Bob, no detectable difference.
- Bob measures result $\uparrow$ or $\downarrow$ at random.
- 25% of time Bob measures $\downarrow$.
- Alice & Bob see, there's a problem.

Quantum computer

- Use techniques of quantum theory to analyze protocols like BB84 (polarized photons implement qubits, "quantum bits").
- Exploit "entanglement" between qubits (e.g. Ekert E91 protocol).

Quantum computer

- Uses quantum bits instead of ordinary bits.
- Each has continuous range of states (like polarization of photon).
- Various ways to measure (read) it, but only two possible results.
- Computation: various operations, then measure.
- Essentially probabilistic, but can still get tight results.
- Hard to build! E.g., photons won't stay still.
Shor's algorithm
- Efficient quantum algorithm to factorize large numbers
- Works by clever use of number theory and Fourier transform
- Probably get answer quickly - then can check it.
- Existing quantum computer to factorize 15
- We're nowhere close to scaling it up yet
- If we do, it will break RSA

Quantum computing & cryptography
- Basic principles of quantum mechanics
- A selection of quantum algorithms & protocols
- Principles & consequences of quantum cryptography
- Prospects for future progress

Main text book
Quantum Computer Science: An Introduction
David Mermin
Cambridge University Press 2007