Quantum computing & cryptography

Week 4

Cryptographic protocols
- Quantum key distribution
- Bell states for entanglement
- Bit commitment

Cryptography

One party to send secret message to another

Alice
- e.g. you & your bank

Bob
- Current technology
- Public key cryptography —
  - To encrypt: need to know key
  - To decrypt: need to know how key was constructed

e.g. RSA

Key \( N = \text{product of two large primes} \ p, q \)

\( N \) is public — Any one can encrypt.

Bob knows \( p, q \) — he decided \( p, q \) first,
  then calculated \( N = pq \)

\( \therefore \) Bob can decrypt

For anyone else to decrypt, they must work out \( p \) and \( q \) from \( N \) — HARD. Takes too long
BUT quantum computers would make it easy
  - Then RSA not secure any more 😞

Quantum channels

Qbit = polarized photon
Transmission — along fibre optic cable
Wave picture: light waves vibrate in all directions
Polaroid filter
- passes light vibrating one direction
- stops it for other direction

Polarized light

Unpolarized light

Second filter at 90° will stop light altogether

Also: birefringent crystal sends different polarizations in different directions

Birefringent crystals

Hello!

Light → polarized

Text viewed through birefringent calcite crystal (Iceland spar)

Calcite in the refraction test

You will require

From: Wikipedia (Furfi)

Viking "sunstone"?

Polarization states as qubit states

Hadamard axis

Y-axis points are circular polarization
One-time pads

- Alice wants to send Bob a message of $N$ bits $M_0, M_1, \ldots, M_{N-1}$
- They already both know a secret random string of $N$ bits $S_0, S_1, \ldots, S_{N-1}$
- Alice encrypts her message as $(M_0 \oplus S_0, M_1 \oplus S_1, \ldots, M_{N-1} \oplus S_{N-1})$
- Bob decrypts it as using $M_i = M_i \oplus S_i \oplus S_i$

Eavesdropping

EVE sees a random string $(M_0 \oplus S_0, M_1 \oplus S_1, \ldots, M_{N-1} \oplus S_{N-1})$

Tells her nothing about message.

BUT Alice & Bob can't reuse their one-time pad for another message $M_0', M_1', \ldots$

If they did, Eve could calculate $M_i \oplus M_i' = (M_i \oplus S_i) \oplus (M_i' \oplus S_i)$

- not so random
- Statistics based on message type
  $\Rightarrow$ information about messages & pad

Quantum key distribution (QKD)

Using quantum channel to agree one-time pad

Alice $\rightarrow$ Bob:

- long (>2N) stream of qubits
- prepares each randomly as:
  - type 1: $\{ |0\rangle, |1\rangle \}$ code 0
  - type H: $\{ |H\rangle |0\rangle, |H\rangle |1\rangle \}$ code 1

BB84 - Bennett, Brassard 1984

When Bob receives each qbit:

1. Randomly applies $I$ or $H$
2. Measures qbit
- 4 combinations of operators on original $|\rangle$

Alice       Bob        Final state  Bob's measurement

$|0\rangle$ $|$1$ |I\rangle$ $|\rangle$   random: $|0\rangle$
$|0\rangle$ $|H\rangle$ $|H\rangle$ $|\rangle$   random: Useless qbits
$|1\rangle$ $|I\rangle$ $|H\rangle$ $|\rangle$   random: Useless qbits
$|1\rangle$ $|H\rangle$ $|H\rangle$ $|\rangle$   random: Useless qbits
Next

- Alice tells Bob the types (1 or H) she gave to all the qubits.
- Bob tells Alice which of those are useful (because he used the same gate as Alice).
- Then they both know which qubits were useful & what values (0 or 1) they were.
- These values make up the one-time pad.

**What can Eve do?**

1. Eve knows what type each qubit is:
   - intercept qubits
   - apply 1 or H as appropriate
   - measure qubits - find values
   - recreate qubits & send to Bob

E.g. Type H:

```
<table>
<thead>
<tr>
<th></th>
<th>Alice</th>
<th>Eve</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Eve can use the qubits to create random values and send them to Bob. Bob then compares these values to the ones Alice sent. If they match, Bob knows the qubits were not intercepted. If they do not match, Bob knows the qubits were intercepted.

Eve can also try to guess the type of each qubit. However, without knowing the type, Eve cannot be sure if the qubits were intercepted or not. Bob can verify the qubits by comparing the received values with the expected values.
Other 50%: Eve guesses wrong

\[ |0\rangle \quad \text{or} \quad |1\rangle \]

Later, Eve intercepts insecure channel, discovers
- That was a useful bit
- Her value 0 or 1 is random
- She might have changed qubit state \( |x\rangle \)

... In 25% of useful qubits: Eve's interception \( \Rightarrow \) Bob gets wrong bit

Alice & Bob protect themselves

- Test qubits
- Sacrifice some useful qubits
- Use them to detect interception
- Use classical channel to communicate their values sent/received

\[ \text{discrepancy} \Rightarrow \text{interception} \]

25% discrepancy suggests 100% interception

smaller discrepancy \( \Rightarrow \) lesser security breach

next week: see how to deal with that

If no discrepancy: what do you deduce?

Bound on interception rate
- But certainty depends on number of qubits
  
  \[ \binom{15}{10} \]
  
  Want \( \binom{15}{10} \leq 0.01 \)

\[ n > \frac{\log 0.01}{\log 0.99} \approx 7 | \]

What can Eve do?

Use quantum computer?

Idea

\[ |\psi\rangle \quad \text{State from Alice} \quad \begin{array}{c} \text{Same state} \quad \text{to Bob} \end{array} \]

Eve's computer

\( \{ \phi^T, \mu = 0, 1, 2, 3 \} \) are \( \{ 0^T, 1^T, H | 0^T, H | 1^T \} \)

Hope: can get 4 states \( |\mu\rangle \) whose differences give information about \( \mu \)

\[ \langle \phi^T | \phi^T \rangle \text{inner product} \]

For \( \mu \in 0.02, 0.03, 0.12, 0.13 \)

\[ \langle \phi^T | \phi^T \rangle = 1 \]

\[ \langle \mu | \mu \rangle = 1 \quad \langle \mu | \mu \rangle = 1 \quad \langle \mu | \mu \rangle = 1 \]

\[ \langle \mu | \mu \rangle = 1 \]

\[ \langle \mu | \phi^T \rangle = 1 \]

\[ \langle \mu | \phi^T \rangle = 1 \]

\[ \langle \mu | \phi^T \rangle = 1 \]

\[ \langle \mu | \phi^T \rangle = 1 \]
Summary

- Alice & Bob use quantum channel to agree a one-time pad of random bits
- They can’t transmit a meaningful message that way (lose half the bits)
- But they can use the one-time pad to encrypt a message on an insecure channel
- Any interception (Eve) on the quantum channel can be detected.

QKD: current achievements

- Fastest: 1 Mbit/s (20 km fibre)
- 10 kbit/s (100 km fibre)
- 2007

- Furthest: 148 km (fibre)
- 144 km (open air)
- Suggests further beyond atmosphere e.g. satellite communication

- Commercially available
  - several companies & networks

The Bit Commitment problem

Alice must make a decision (YES/NO) today and prove to Bob she has done so. But she doesn’t want Bob to know what the decision was until tomorrow.

TODAY

TOMORROW
Quantum Bit Commitment

Like BB84

Like one-time pad: Alice sends Bob n Qubits today but ALL Alice's Qubits are:

\begin{align*}
\text{type } \{ \frac{1}{\sqrt{2}} | \text{H} \rangle \text{ if she decided } \{ \text{YES} \} \\
\text{NO} \}
\end{align*}

Tomorrow: Alice tells Bob how she prepared all the Qubits.

Bob's useful measurements are where his type agrees with Alice's.

For them, his values should match what Alice tells him. If so, he believes Alice.

e.g. if Alice decides NO

Today:

\begin{align*}
\text{Alice prepares } |0\rangle, |1\rangle, |H\rangle, |H\rangle, |0\rangle, |0\rangle, |0\rangle, |H\rangle
\end{align*}

Bob's gate:

\begin{align*}
\text{Bob measures } & 1, 0, 1, 1, 1, 1, 1, 0
\end{align*}

Useful

Tomorrow:

\begin{itemize}
  \item Alice tells Bob how she prepared qubits.
  \item For qubits where Bob used H, what she says matches his measurements.
  \item Probability of that happening by chance.
\end{itemize}

What happens if Alice lies?

What if she changes her mind?

Can she persuade Bob she decided yes?

Alice knows Bob's H measurements.

Wants to pretend she knows his |1⟩ measurement.

But she can only guess.

Similarly if she starts undecided, prepares Qubits of both types (|1⟩ and |H⟩).

Can Bob cheat?

Can he get information today about Alice's decision?

No!

Situation: Every qubit randomly prepared in one of two orthonormal states |1⟩, |0⟩.

Can Bob get information about what were two states?

\begin{itemize}
  \item Measure every qubit.
  \item Probability of 0 = \frac{1}{2} |0⟩|0⟩ + \frac{1}{2} |1⟩|1⟩.
  \item But |0⟩, |1⟩ are amplitudes for |0⟩.
  \item w.r.t. basis |0⟩, |1⟩
  \item 10⟩ = |0⟩|1⟩ + |1⟩|0⟩.
  \item |0⟩|0⟩ + |1⟩|1⟩ = 1
  \item Probability of 0 = \frac{1}{2}.
\end{itemize}

\begin{itemize}
  \item Whatever |0⟩, |1⟩ are
\end{itemize}
Protocol in Mermin

Today: Bob stores qubits when he receives them
Tomorrow: Alice tells Bob her decision
  • Bob applies corresponding gate to all the qubits

Advantage: All qubits useful
  • higher degree of confidence in Alice
Disadvantage: Storing qubits is beyond current technology
  (e.g. for polarized photons)

Can Alice cheat?

Yes, unfortunately.
  - but she needs to be able to
    1) store bits,
    2) entangle bits

Bell states

$$|\psi_{xy}\rangle = \frac{1}{2}(|00\rangle + |11\rangle)$$

E.g. $$|\psi_{xx}\rangle = \frac{1}{2}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(10\rangle + 11\rangle)$$

Entangled

Measuring either qubit equally likely to give 0 or 1
  but other must give the same.

Getting $$|\psi_{xy}\rangle$$ from $$|\psi_{00}\rangle$$

$$|\psi_{xy}\rangle = C_{xy} H |x y\rangle = C_{xy} H X_{xy} X_0 |00\rangle$$

= $$C_{xy} Z_{xy} H_{xy} |00\rangle$$

= $$Z_{xy} X_{xy} C_{xy} H_{xy} |00\rangle$$

= $$Z_{xy} X_{xy} |\psi_{00}\rangle$$

:. other Bell states got from
  $$\frac{1}{\sqrt{2}} (10\rangle + 11\rangle)$$ by flipping one qubit, changing + to - , or both.

Note: $$Z_0 |\psi_{00}\rangle = Z_1 |\psi_{00}\rangle$$

$$Z_1 X_0 |\psi_{00}\rangle = X_0 Z_1 |\psi_{00}\rangle$$

$$X_1 X_0 |\psi_{00}\rangle = X_0 Z_1 |\psi_{00}\rangle$$
Bell states and Hadamard

\[ H, H_0 |\psi_{oo}\rangle = |\psi_{oo}\rangle \]

Week 2:

\[ H \quad H \quad H \quad H \]

\[ \times \quad \times \quad H \]

\[ |\psi_{oo}\rangle = H_0 H |\psi_{oo}\rangle 
\]

\[ = C_{01} H_0 |100\rangle \quad \text{with two qubits swapped} \]

\[ = |\psi_{oo}\rangle \quad \text{symmetric in two qubits} \]

Alice cheats at bit commitment

Today: Alice makes \( n \) pairs of qubits
- entangles each pair in Bell state \( |\psi_{oo}\rangle \)
- sends right half of each pair to Bob

State of pair is \[ \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle) \]

Type 1 measurement:
If Bob does (partial) measurement on qubit 0:
- state goes to \( |10\rangle |0\rangle \) with prob. \( \frac{1}{2} \)
- \( |01\rangle |1\rangle \)

\[ \frac{1}{2} \]

Type 2 measurement:
If Bob does \( H \) before measuring, state becomes
\[ H_0 |\psi_{oo}\rangle = |\psi_{oo}\rangle \]

\[ H_0 |\psi_{oo}\rangle = |\psi_{oo}\rangle \]

\[ = \frac{1}{\sqrt{2}} H |10\rangle |0\rangle + \frac{1}{\sqrt{2}} H |1\rangle |1\rangle \]

On measurement by Bob, this goes to
- \( H |0\rangle |0\rangle \) with prob. \( \frac{1}{2} \)
- \( H |1\rangle |1\rangle \) with prob. \( \frac{1}{2} \)

Exercise: calculate explicitly with \( \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \)

Alice cheating

She applies \( 1 \) or \( H \) to all her qubits
- measures them
- reports the results to Bob.

Suppose she decides yes & applies \( 1 \)

Where Bob did type 1 measurement:

<table>
<thead>
<tr>
<th>Bob's value</th>
<th>state</th>
<th>Alice's measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>0\rangle</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>1\rangle</td>
</tr>
</tbody>
</table>

Alice discovers exactly what Bob measured
Where Bob did type H measurement: Alice cheating

<table>
<thead>
<tr>
<th>Bob's value</th>
<th>state</th>
<th>Alice's measurement value</th>
<th>prob</th>
<th>new state</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$</td>
<td>0\rangle\otimes</td>
<td>0\rangle\rangle$</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>$</td>
</tr>
<tr>
<td>1</td>
<td>$</td>
<td>1\rangle\otimes</td>
<td>1\rangle\rangle$</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>$</td>
</tr>
</tbody>
</table>

Alice knows nothing about Bob's value.
In both cases, Alice knows exactly what she would have known about Bob's value if she hadn't cheated.

Similarly if Alice decides No

Alice cheating

She - applies H to all her qubits
- measures them
- reports results to Bob
Where Bob had applied 1:
State $|0\rangle|0\rangle$ or $|1\rangle|1\rangle$ → $H|0\rangle|0\rangle$ or $H|1\rangle|1\rangle$
Measurement gives random result.

Where Bob had applied H:
State $H|1\rangle|0\rangle$ or $H|0\rangle|1\rangle$ → $|00\rangle$ or $|11\rangle$
Measurement gives Bob's value.

Alice honest:

Alice prepares $|1\rangle|0\rangle\rangle\rangle\rangle\rangle\rangle\rangle$ = Alice prepares
Bob's gate
Bob measures

Alice cheats:

Alice prepares $\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$
Bob's gate
Bob measures
State
Alice decides $H$ measures
decides $H$, measures $|?\rangle|?\rangle$ $|?\rangle$ $|?\rangle$ $|?\rangle$ $|?\rangle$