Quantum Computing and Cryptography

Week 5
Cryptography issues

AKK: quantum key distribution

Not in Mermin.

Steve Vickers

What does BB84 achieve?

No passive eavesdropping

- Eve cannot gain information without disturbing the messages.

Physics prevents this.

cf. for classical messages:

one-time pad: locked in box, sent by courier
To read it: wait till courier is asleep; pick lock, copy pad

Not easy! But laws of physics don't forbid it.

Information gain => disturbance?

Not true for orthogonal states, e.g. |0⟩, |1⟩

If message qubit known to be either |0⟩ or |1⟩,

can find out which without disturbing message

Use it as control for (NOT):

\[ \text{Eve: } |0⟩ \xrightarrow{\times} |1⟩ \]

message \[ |1⟩ \xrightarrow{\times} |1⟩ \]

\[ \text{CNOT: } |0⟩|1⟩ \xrightarrow{\times} |1⟩|1⟩ \]

- entangled - Eve can measure her qubit without affecting message

\[ \text{Doesn't extend to other message states} \]

\[ |ϕ⟩ = α |0⟩ + β |1⟩ \]

\[ \text{CNOT: } |0⟩|ϕ⟩ = α |0⟩|0⟩ + β |1⟩|1⟩ \]

- entangled

If Eve measures her qubit, that changes the state of the message.

Equivalent to:

\[ \text{Eve measures} \]

message \[ |ϕ⟩ \xrightarrow{\text{Eve measures}} |0⟩ \text{ or } |1⟩ \]
Information gain ⇒ disturbance  True in general

Suppose two possible message states \( |\psi\rangle, |\phi\rangle \)
not orthogonal: \( \langle \psi | \phi \rangle \neq 0 \)

Eve's aim:
- prepare extra ("ancilla") state \( |u\rangle \)
- apply unitary operation \( U \) to \( |u\rangle \) message
- get unentangled state where message is undisturbed, but ancilla distinguishes \( |\phi\rangle \) from \( |\psi\rangle \)

Eve: \( |u\rangle \)
message: \( U \)
message unchanged

\[
U |u\rangle |\phi\rangle = |u\rangle |\psi\rangle \\
U |u\rangle |\psi\rangle = |u\rangle |\phi\rangle
\]

message undisturbed \( \psi, \psi' \) distinguish message states

Inner product of \( |u\rangle \langle u| |\psi\rangle \) with \( |u\rangle \langle u| |\phi\rangle \)
\[
= \langle u | u \rangle \langle \psi | \phi \rangle \quad \text{"Can prove as general result for inner products of tensors"}
\]

But also =
\[
= \langle u | u \rangle \langle u | u \rangle |\phi\rangle = \langle \psi | \phi \rangle \quad \text{U unitary}
\]

\[
= \langle u | u \rangle = 1 \quad \text{using } \langle u | u \rangle = 0
\]

\[
\langle u | u \rangle = 1 - \text{so } \psi, \psi' \text{ don't distinguish } |\psi\rangle \text{ from } |\phi\rangle
\]

Dealing with disturbance

Previous discussion:
Eavesdropping ⇒ disturbance
⇒ discrepancy in 25% of disturbed test qubits
⇒ No discrepancy
⇒ confidence level of no eavesdropping

Suppose there is a discrepancy?

Two sources of disturbance

0 Eavesdropping
1 Channel noise

\{ can't tell them apart

Channel noise - fact of life
\( \text{True also for classical channels, e.g. internet} \)
⇒ likely to get discrepancies even without eavesdropping.
Two consequences of disturbance

1. Transmission errors.
   Discrepancies in test qubits
   \[ \Rightarrow \] similarities in discrepancies likely in qubits "good" for key
   Must remove these (information reconciliation = error correction)
   Privacy amplification

2. Information might have leaked out (to Eve)
   - How much? Estimate upper bound from test qubits
   Can minimize the impact of this

Information reconciliation = error correction

There are techniques for quantum error correction
- but rely on quantum computation
- still in the future

Doesn't matter!
- Alice & Bob can do it over classical channels
- If Eve can intercept the classical messages, more information leaks to her
- Alice & Bob can allow for that

The problem
Test qubits show discrepancies in \( \times \% \) of good qubits
Bob's measurement type = Alice's preparation type

\[ \therefore \] expect about \( \times \% \) of keys to have discrepancies

Alice's key
Bob's

mostly agree

Finding the discrepancies
Simplified version

e.g. Suppose 1 discrepancy expected in 16 bits
Alice & Bob tell each other parities of blocks of bits

Alice
Bob

Block
Alice parity
Bob parity
Binary search:

1-15
0-7
0-3
4-5
4

0
1
0
0
1
1
0
0
1
0
1
1
1
1
1
1
1
1
**Information leakage**

Reconciliation is over classical channel. Eve may eavesdrop. Each parity reveals one bit's worth of information to Eve.

E.g. previous slide:
- Started with 16 bits
- Revealed 5
- 11 bits' worth left

**Can counteract leakage**

discard last bit of each block whose parity is revealed
- Then Eve has no information about the rest

At the end, the error has definitely been discarded
- don't need to exchange bits 4 - discard it anyway

**General situation**

- Partition bits into blocks of size \( k \) such that each block is unlikely to have more than one discrepancy
- Reveal parities of blocks - leaks 1 bit per block
- For each block with parity discrepancy, binary search to find bit discrepancy
  - leaks \( \log_2 k \) bits per block searched
- Counteract leakage by discarding a bit from each block whose parity is revealed
- Repeat until low risk of further errors

**Simplest case: \( k = 2 \)**

Even block \( \vee \vee \) or \( xx \): discard 2nd bit \( x \)

\[ v = B \& A \text{ agree} \quad x = \text{discrepancy} \]

Odd block \( \vee x \) or \( xx \): discard both bits

\[ \text{parities disagree (could be 2 discrepancies cancel)} \]

\[ \text{parities agree} \]

Suppose \( p = \text{prob. of discrepancy (error rate)} \)

Prob. odd block = \( 2p \) \( (1-p) \)

On average per block:
- Lose \( 1 + 2p(1-p) \) bits
- Lose \( \geq 2p(1-p) \) errors
\( p = 0.2 \) (20% error)

\[
\text{prob. odd block} = 2 \times 0.2 \times 0.8 = 0.32
\]

In 1000 bits: expect 200 errors

500 blocks: expect 170 odd blocks

\( \sim \frac{330}{2} \) remain

\( \text{Error rate now} \sim \frac{330}{330} \sim 10\% \)

\[
\text{Cost per error bit removed}
= \frac{1 + 2p(1-p)}{2p(1-p)} \text{ bits}
\]

<table>
<thead>
<tr>
<th>( p )</th>
<th>cost per error</th>
</tr>
</thead>
<tbody>
<tr>
<td>20%</td>
<td>4.1</td>
</tr>
<tr>
<td>10%</td>
<td>6.5</td>
</tr>
<tr>
<td>5%</td>
<td>11.5</td>
</tr>
<tr>
<td>1%</td>
<td>51.5</td>
</tr>
</tbody>
</table>

Need bigger blocks to get benefit of binary search.

In general

\[
\text{error rate } p, \text{ block size } k
\]

\[
\text{Prob. odd block} = \frac{1 - (1 - 2p)^k}{2}
\]

Typically, \( k \frac{1}{2} \) for suitable \( k \)

For each even block: lose 1 bit

For each odd block: lose \( k \) bits including at least one error

You don't have to know this!

Proof of Prob. odd block

\[
\text{Prob. odd block} = \frac{1 - (1 - 2p)^k}{2}
\]

\[
\text{Prob. } i \text{ errors in block} = \binom{n}{i} p^i (1-p)^{k-i}
\]

\[
\text{Prob. odd block} = \sum_{i=0}^{k-1} \binom{n}{i} p^i (1-p)^{k-i} = P_0 \text{ (say)}
\]

\[
\text{Prob. even block} = \sum_{i=0}^{k} \binom{n}{i} p^i (1-p)^{k-i} = P_e \text{ (say)}
\]

\[
P_0 + P_e = \sum_{i=0}^{k-1} \binom{n}{i} p^i (1-p)^{k-i} + \binom{n}{k} p^k (1-p)^{k-k} = (p + 1-p)^k = 1
\]

\[
-P_0 + P_e = \sum_{i=0}^{k} \binom{n}{i} p^i (1-p)^{k-i} - \binom{n}{k} p^k (1-p)^{k-k} = (p - 1+p)^k = (-2p)^k
\]

\[
P_0 = \frac{1 - (-2p)^k}{2}
\]

\begin{tcolorbox}
\emph{binomial theorem}
\end{tcolorbox}
e.g. \( p = 0.01, k = 64 \) = \( 2^c \)
Prob. odd block = \( 1 - 0.98^{64} \) = 0.36

In 1024 bits: expect \( \sim 10 \) errors,
16 blocks: expect \( \sim 6 \) odd blocks
10 even
Lose 16 + 6 x 6 = 52 bits, leaving 972
Remove 6 errors, leaving 4

After 3 or 4 more iterations, error should be gone
- no odd blocks found
- extremely low probability of two errors in some block

**How much might Eve know?**
- Test qubits show discrepancies in \( p \) % of good qubits
- Have to assume that’s because of eavesdropping
  (because we can’t distinguish it from noise)
- Suggests Eve intercepts \( 4 \times \) % of qubits
- In about \( \frac{1}{2} \) of those – \( 2 \times \) % – she measured
  with correct type and hence knows bit
- Eve may have learned from reconciliation

Suppose she knows \( e \) bits’ worth in total

---

**After information reconciliation**

Alice and Bob each have a string of \( n \) (say) bits.
To a high probability, they are equal - \( X \), say

**very small prob. that reconciliation missed error**

**How much might Eve know?**

We assume Eve can intercept all classical communications

- e.g. Eve knows Alice & Bob’s preparation & measurement types
- she knows which of her own measurements matched Alice & Bob’s good bits

---

**Privacy amplification**

Alice & Bob’s string \( X \) has \( n \) bits
Eve maybe knows \( e \) bits,
- but Alice & Bob don’t know which

There are \( \sim 2^{n-e} \) strings matching Eve’s knowledge

Idea: apply a random hash function \( h \)
 reducing \( n \) bits to \( m \leq n-e \)
Alice & Bob use \( h(X) \) as their key.
If \( G \) distributes Eve’s \( 2^{n-e} \) possibilities evenly
over \( 2^m \) m-bit strings, then her knowledge is scrambled.
Universal hash functions \( n \)-bit strings \( \rightarrow \) \( m \)-bit strings

Have a collection \( G \) of hash functions \( g \)

- if \( a_1, a_2 \) are any two distinct \( n \)-bit strings
- choose \( g \) at random (uniformly)

Then \( \text{prob} (g(a_1) = g(a_2)) \leq \frac{1}{2^m} \)

such collections are publicly available

Probabilities

Suppose you had two random \( n \)-bit strings, \( X \) and \( Y \), independent and with the same distribution as our \( X \).

\[ \text{prob} (X = Y) = \frac{1}{2^n} \]

Now suppose \( Y \) is conditional on what Eve knows.

Eve would like conditional probability

\[ \text{prob} (X = Y | \text{what Eve knows}) = 1 \]

Then what she knows is enough to determine \( X \)

She actually has

\[ \text{prob} (X = Y | \text{what Eve knows}) \leq \frac{1}{2^{n-e}} \]

Probability \( \leftrightarrow \) amount of information

\[ \text{Take } - \log_2 \text{ e.g. } - \log_e \frac{1}{2^m} = k \]

Situation \( \text{prob} (X = Y | \text{what Eve knows}) - \log_2 \text{ collision entropy} \)

Initially \[ \frac{1}{2^n} \]

In Eve's dreams \[ 1 \]

After A-B exchange \[ \frac{1}{2^{m-e}} \]

Third column ("collision entropy")
- Eve's uncertainty, measured in bits
- Reduces calculation to one of probability theory

Theorem on collision entropies

Suppose collision entropy \( d = n-e \)

for \( X \) (given what Eve knows)

Also, \( G \) a class of universal hash functions

Then collision entropy for \( G(x) \)
(given what Eve knows) \( e \) \( G \) chosen uniformly at random

is \[ \geq m - 2^{m-d} \]
Choosing \( m \)

- A & B use \( G \) to hash \( n \) bits into \( m \).
- Eve possibly knew \( e \) bits of \( X \).
- Eve's possible knowledge of \( G(X) \) could be \( 2^{m-e} \) bits.
- Make \( m \) small.
- Eve's possible knowledge is \( n-e \).
- Make Eve's knowledge of \( G(X) \) small at the cost of getting a shorter key.

Security of BB84

- A & B agree on a security parameter \( s, \ell \).
- Probability of success \( \geq 1 - \frac{1}{2}^{2\ell} \) covers small probability that A & B might get different keys.
- Eve's knowledge of final key \( < \frac{1}{2}^{\ell} \).
- It's been proved that BB84 can satisfy any \( s, \ell \) but an abort threshold depends on them.

General scheme of BB84

- Alice sends qubits to Bob.
- They exchange preparation/measurement types.
- They exchange measured values of test qubits.
- If too many discrepancies, abort and try again.
- Information reconciliation.
- Privacy amplification.

Attacks on QKD

- Photon number splitting

  How do you get a single photon?

  Laser normally emits many photons per pulse.

  Turn it down to get at most one per pulse.

  Mostly - no photon at all. A & B wait.
  Sometimes - one photon. A & B use it.
Attacks on QKD ① Photon number splitting

BUT - occasionally ≥2 photons in a pulse
- A&B don't notice. Other photon (in same
  state) unaffected
- Eve waits for A&B to say what type it was
- if it's a good qubit, she can measure it and
  learn a bit of the key

Attacks on QKD ① Photon number splitting

Even worse: Eve could block the single photons
- so she has a copy of all Bob's photons
- or Eve can get some single photons through
  to conceal her activities
A&B know (afterwards) Alice sent photons that
Bob never received
- but that happens anyway even without Eve

Attacks on QKD ② Denial of service

Eve

Alice

Bob

Scissors

glass fibre

But - not passive (A&B find out what
happened)
- not eavesdropping (E learns nothing)

Attacks on QKD ② Denial of service

Eve

Alice

Bob

Scissors

glass fibre

But - not passive (A&B find out what
happened)
- not eavesdropping (E learns nothing)
Attacks on QKD

3. Man in middle

If Eve can impersonate A & B on quantum & classical channels
she can control entire interaction

Limitations

Alice & Bob can send each other messages secure from interception

BUT how do they know they are talking to each other?

_e.g._ if Bob is Alice’s bank

\[ \text{Alice} \rightarrow \text{Eve} \rightarrow \text{Bob} \]

\[ \text{Alice} \rightarrow \text{Eve} \rightarrow \text{Bob} \]

Eve hacks Alice’s account

Eve phishes for account details

Still need passwords, certificates, etc.

Some of these use RSA etc.

Not all can be replaced by quantum protocols.

Limits to quantum cryptography

Can do QKD, can’t do bit commitment
With bit commitment, could also do
- oblivious transfer
  (server sends one out of n pieces of information to client, without knowing which it was & without divulging others)
- secure multiparty computation
  (parties jointly compute a result without learning any more than the result tells them)
  _e.g._ 2 billionaires calculate who is richer without divulging their actual wealth

Summary

- QKD has unique advantage: no passive eavesdropping
- In real QKD do get discrepancies
- Must deal with them - need both reconciliation and privacy amplification (lose key bits)
- Photon number splitting a serious issue - but there are ways to deal with it
- QKD doesn’t solve man-in-middle problem
- How do you know the person at the other end of the quantum channel is who you think it is?