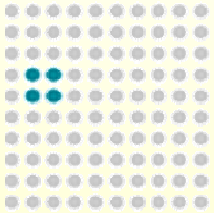
Quantum Cryptography

Stephen Bartlett

Centre for Advanced Computing – Algorithms and Cryptography

Australian Centre of Excellence in Quantum Computer Technology

Macquarie University, Sydney, Australia



CENTRE FOR
QUANTUM COMPUTER
TECHNOLOGY

AUSTRALIAN RESEARCH COUNCIL SPECIAL RESEARCH CENTRE

Lecture 5 on Quantum Computing

NITP Summer School 2003

Adelaide, Australia

28-31 January 2003

Questions in communication

- How much information can be transmitted down a perfect channel?
  - Classical information (how much compression?)
  - Quantum states in a quantum channel
  - Classical information in a quantum channel
  - What types of information can be transmitted?
- What can be done if the channel is noisy?
  - Redundancy/error correction
  - Can quantum mechanics assist a noisy channel?
- How susceptible is the channel/information to eavesdropping?
  - Can we perform secure communication?

Using quantum mechanics in communication

Two non-classical properties of quantum mechanics can help with communication:

- Information gain vs. disturbance
  - Every measurement disturbs the state
  - No measurement on an unknown state can completely determine the state
  - No cloning: quantum information cannot be copied
- Non-classical correlations
  - Entangled states (such as Bell states) carry nonlocal correlations that contradict local realism (Bell's inequalities)

Cryptography

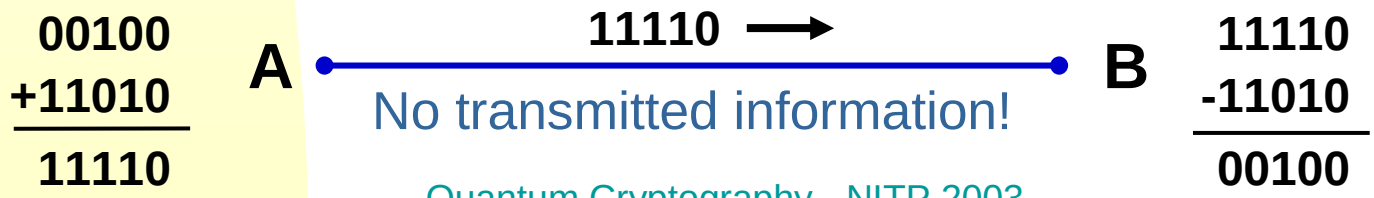
- **A**lice wants to send a message to **B**ob, without an eavesdropper **E**ve intercepting the message
- Public key cryptography (e.g., RSA):
  - security rests on assumptions about comp. complexity
  - vulnerable to attacks by a quantum computer!
- Quantum mechanics provides a secure solution with *quantum key distribution* (QKD)

Private Key Cryptography

- Private key cryptography can be provably secure
  - Alice has secret encoding key *e*, Bob has decoding key *d*
  - Protocol: message *x*, functions *E(x,e)* and *D(y,d)* s.t.

$$D(E(x,e),d) = x$$

- E.g.: one-time pad (*e*=*d*, random string as long as *x*)



Problems with private keys

- How are the private keys distributed?
  - Security rests on private keys being kept secret

Trusted courier?

- Ideally, **A** and **B** wish to generate strings of random numbers *secretly* and *nonlocally*
- Privacy amplification and information reconciliation can be applied to make near-perfect private keys

Using quantum mechanics

- Information gain implies disturbance:
  - Any attempt to gain information about a quantum system *must* alter that system in an uncontrollable way
- Example: non-orthogonal states of a qubit

Eve receives a qubit that is either in $|0\rangle$ or $|+\rangle$

Measure in $|0\rangle, |1\rangle$ basis?

Always gets $|0\rangle$ right, leaves state in $|0\rangle$

50% chance will mistake $|+\rangle$ for $|0\rangle$

Collapses $|+\rangle$ into $|0\rangle, |1\rangle$ basis Disturbance!

Measure in $|+\rangle, |-\rangle$ basis? Similar result

- Information gain by Eve causes an uncontrollable disturbance

BB84 QKD Protocol

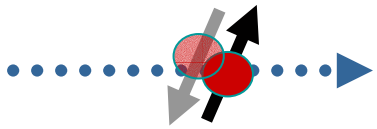
- **1984:** Bennett and Brassard
- Alice generates two random bits, a_1, a_2
- Alice prepares a qubit as follows:

bits	state
00	$\|0\rangle$
01	$\|1\rangle$
10	$\|+\rangle$
11	$\|-\rangle$

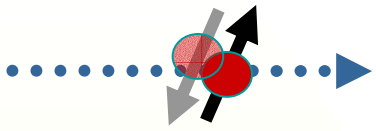
a_1 determines which basis

a_2 is an encoded bit in that basis

- Alice then sends the qubit to Bob



BB84 QKD Protocol



a_1	b_1	?
0	0	✓
1	0	✗
1	1	✓
0	1	✗
1	1	✓
0	0	✓

- Bob receives the qubit
- Bob chooses a random bit b_1 and measures the qubit as follows:
  - if $b_1=0$, Bob measures in the $|0\rangle, |1\rangle$ basis
  - if $b_1=1$, Bob measures in the $|+\rangle, |-\rangle$ basis

  obtaining a bit b_2
- Alice and Bob publicly compare a_1 and b_1
  - if they are the same (Bob measured in the same basis that Alice prepared) then $a_2=b_2$
  - if they disagree, they discard that round

This protocol is repeated $(4+\delta)n$ times

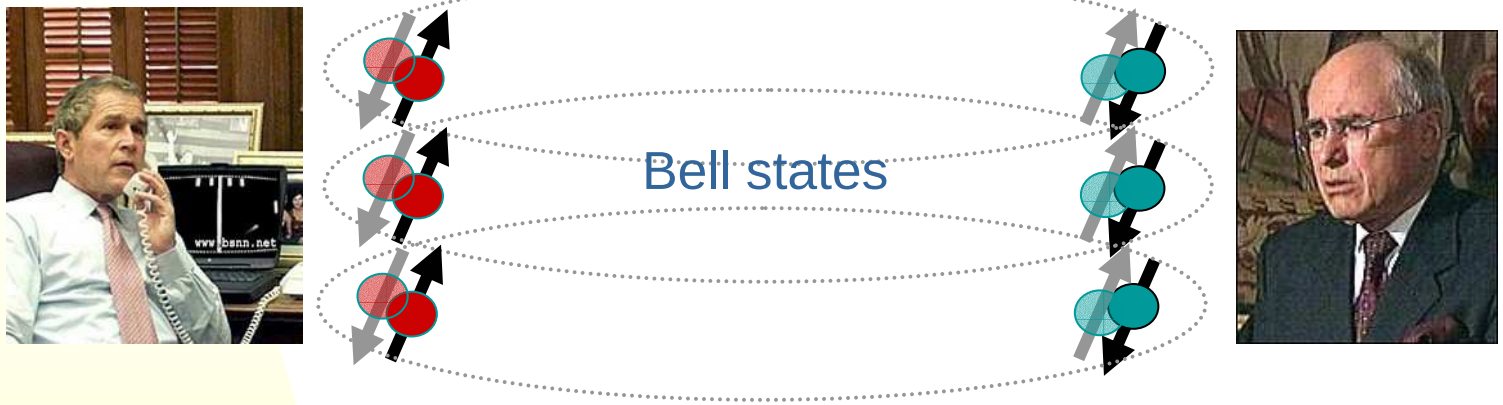
BB84 QKD Protocol

- With high probability, Alice and Bob have *2n* successes
- To check for Eve's interference:
  - Alice chooses *n* bits randomly and informs Bob
  - Alice and Bob compare their results for these *n* bits
  - If more than an acceptable number disagree, they abort

    $\rightarrow$ evidence of Eve's tampering (or a noisy channel)
- Alice and Bob use the remaining *n* bits as a private key!

Ekert's QKD Protocol

- 1991: Artur Ekert presented an equivalent protocol



- Alice and Bob share Bell states
  - For each pair, they both measure randomly in the $|0\rangle, |1\rangle$ or $|+\rangle, |-\rangle$ bases
  - They compare which bases they measured in
  - If they agree, they have correlated random numbers

Two-party protocols

- Not all cryptography involves secret messages
- Consider two parties who don't *trust* each other:

  - You and your "bank" on the internet: Is it your bank?
  - You and an online casino
  - You and your spouse during a divorce

- Cryptography also studies *the protection of private information in the midst of public decision*

Two-party protocols

- Example 1: Internet gambling
  - You play roulette on an online casino
  - The casino says, “You lose!”
  - How do you know you lost?

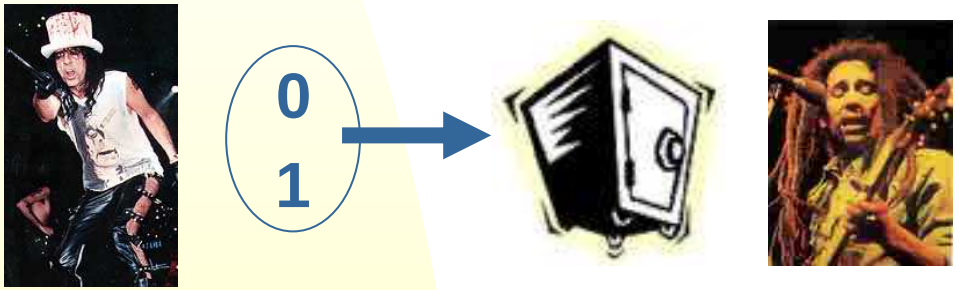
- Example 2: Internet banking
  - You use a website that looks like your bank’s
  - It says, “Please enter your account and password”
  - How do you know it’s really your bank?
- Example 3: The divorce
  - You divorce your spouse, and agree that a coin toss will decide who takes the house and who takes the car
  - You don’t want to meet; can it be done on the phone?

Bit commitment

- Bit commitment is a “primitive” that allows for many two-party protocols to be constructed

Bob wants Alice to “commit” to a bit (a choice 0 or 1)

Alice does not want Bob to know her choice until later



Stage 1: Commitment
Alice chooses a bit, locks it in a safe, and gives the safe to Bob

Stage 2: Unveiling Alice gives the key to Bob, who opens the safe and finds out her choice of bit

Classical bit commitment

- Many cryptographic protocols can be “built” out of bit commitment
- E.g., a coin toss: Alice randomly commits a bit, then Bob guesses her choice
  - If he’s right (50% chance) he wins the toss
  - If he’s wrong (50% chance) he loses

- Unconditional classical bit commitment is impossible!
  - Bit commitment protocols are based on assumptions about computational complexity
  - Vulnerable to attacks (cheating) by quantum computers
- Quantum mechanics: information gain vs disturbance
- Is there a quantum bit commitment?

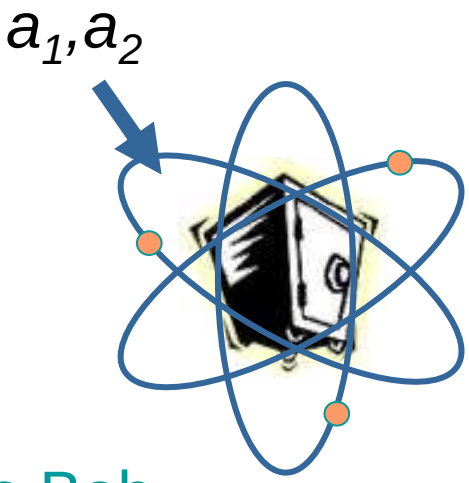
Quantum bit commitment

- Example: Alice chooses a bit a_1 to commit, and a random bit a_2, then prepares a qubit as follows:

bits	state
00	$\|0\rangle$
01	$\|1\rangle$
10	$\|+\rangle$
11	$\|-\rangle$

a_1 determines which basis

a_2 is an encoded bit in that basis

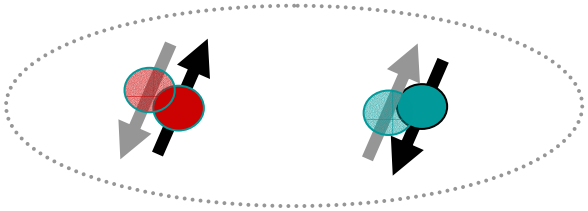


- Commitment: She gives the qubit to Bob
- Bob doesn't know what basis to measure in
- Unveiling: Alice tells Bob a_1 ,a_2, and Bob measures in the correct basis to check her honesty

PROBLEM! Coherent attacks

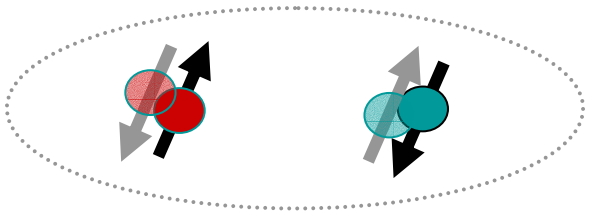
- This example of quantum bit commitment is completely insecure against Alice cheating!
- "Coherent attack": Alice does NOT prepare the required state, but instead prepares a Bell state

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$



with another qubit that she keeps

- No commitment has been made



But Bob doesn't know that Alice is cheating...

Coherent attacks

- At the unveiling phase, Alice chooses her bit then measures the qubit she kept in that basis

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle - |{-}{-}\rangle)$$

  - Chooses **0**: measures in $|0\rangle, |1\rangle$ basis
  - Chooses **1**: measures in $|+\rangle, |-\rangle$ basis
- Alice knows Bob's measurement results will be *correlated* with hers (in either basis)
- She knows exactly what state to tell Bob

Quantum bit commitment is impossible!

Mayers, Lo and Chau (1997)

Summary of quantum crypto

- Information is physical
- Information gain implies disturbance:
  - Any attempt to gain information about a quantum system *must* alter that system in an uncontrollable way
- Use this property to protect information
  - An eavesdropper's attempt to gain information will alter the system and thus may be detected!
- Future attempts to communicate securely or to protect private information in the midst of public decision may rely on quantum physics