Topics 11-13: Quantum cryptography in the presence of noise and adversaries

1. Quantum money
2. Quantum bit commitment (M 6.3)

Topics 11-13: Quantum cryptography in the presence of noise and adversaries

1. Quantum money

2. Quantum bit commitment (M 6.3)

3. Quantum key distribution (NC 12.6, M 6.2)
    - Encryption
    - Classical one-time pad
    - Key distribution problem
    - QKD through a noiseless insecure channel (BB84, E92, and their relation)
    - QKD through noisy insecure channels

Topics 11-13: Quantum cryptography in the presence of noise and adversaries

1. Quantum money

2. Quantum bit commitment (M 6.3)

3. Quantum key distribution (NC 12.6, M 6.2)
    - Encryption
    - Classical one-time pad
    - Key distribution problem
    - QKD through a noiseless insecure channel (BB84, E92, and their relation)
    - QKD through noisy insecure channels

Additional reading: chapter "Quantum cryptology" by Hoi-Kwong Lo in "Introduction to Quantum Computation and Information" by Lo, Popescu, and Spiller.

Cryptography: information processing to protect honest parties from the action of malicious adversaries.

Quantum money (Wiesner late 60's, published 83)

Question: how to make money that cannot be forged?

Cash is made to be physically hard to forge. Its security is based on (unverifiable, potentially mistaken) assumption on the limitations of the adversary.

Quantum money (Wiesner late 60's, published 83)

Question: how to make money that cannot be forged?

Cash is made to be physically hard to forge. Its security is based on (unverifiable, potentially mistaken) assumption on the limitations of the adversary.

A better tomorrow (1985)

Wiesner's idea: use laws of physics to prevent forging!

Usual: each banknote has a unique n-bit serial number c1 c2 ... cn.

Wiesner's idea: use laws of physics to prevent forging!

Usual: each banknote has a unique n-bit serial number c1 c2 ... cn.

New: serial number is stored as an n-qubit quantum state on the banknote: $H^{b_1}|c_1\rangle \otimes H^{b_2}|c_2\rangle \otimes \cdots \otimes H^{b_n}|c_n\rangle$

where b1 b2 ... bn is an n-bit random string.

Wiesner's idea: use laws of physics to prevent forging!

Usual: each banknote has a unique n-bit serial number c1 c2 ... cn.

New: serial number is stored as an n-qubit quantum state on the banknote: $H^{b_1}|c_1\rangle \otimes H^{b_2}|c_2\rangle \otimes \cdots \otimes H^{b_n}|c_n\rangle$

where b1 b2 ... bn is an n-bit random string.

The bank keeps a record of both c1 c2 ... cn and b1 b2 ... bn.

Wiesner's idea: use laws of physics to prevent forging!

Usual: each banknote has a unique n-bit serial number c1 c2 ... cn.

New: serial number is stored as an n-qubit quantum state on the banknote: $H^{b_1}|c_1\rangle \otimes H^{b_2}|c_2\rangle \otimes \cdots \otimes H^{b_n}|c_n\rangle$

where b1 b2 ... bn is an n-bit random string.

The bank keeps a record of both c1 c2 ... cn and b1 b2 ... bn.

To spend the money, the banknote should be verified by the bank who measures in the {|0>,|1>} or the {|+>,|->} basis according to b1 b2 ... bn.

Wiesner's idea: use laws of physics to prevent forging!

Usual: each banknote has a unique n-bit serial number c1 c2 ... cn.

New: serial number is stored as an n-qubit quantum state on the banknote: $H^{b_1}|c_1\rangle \otimes H^{b_2}|c_2\rangle \otimes \cdots \otimes H^{b_n}|c_n\rangle$

where b1 b2 ... bn is an n-bit random string.

The bank keeps a record of both c1 c2 ... cn and b1 b2 ... bn.

To spend the money, the banknote should be verified by the bank who measures in the {|0>,|1>} or the {|+>,|->} basis according to b1 b2 ... bn.

A forger having the banknote alone cannot learn c1 c2 ... cn, b1 b2 ... bn from the quantum state, nor to clone it (cf A4Q1).

Theme:

Exploit the difference between having a copy of a quantum state, and knowing what it is.

Theme:

Exploit the difference between
having a copy of a quantum state, and
knowing what it is.

Conjugate coding:
The bit c is encoded in one of the two conjugate (or mutually unbiased) bases {|0>,|1>} or {|+>,|->}. Measuring in one basis completely destroys the info in the other, so if you have the state but not knowing the basis:
(a) it's hard to learn c
(b) inevitably disturbs the quantum state

Theme:

Exploit the difference between
having a copy of a quantum state, and
knowing what it is.

For Wiesner's quantum money scheme, the limited prob of success to learn each bit of the serial number is bootstrapped to suppress the probability to learn the entire serial #.

Theme:

Exploit the difference between
having a copy of a quantum state, and
knowing what it is.

For Wiesner's quantum money scheme, the limited prob of success to learn each bit of the serial number is bootstrapped to suppress the probability to learn the entire serial #.

Question: is it provable that the probability to learn the n-bit serial # decreases exponentially with n?
(a) Yes, (b) No.

Theme:

Exploit the difference between
having a copy of a quantum state, and
knowing what it is.

For Wiesner's quantum money scheme, the limited prob of success to learn each bit of the serial number is bootstrapped to suppress the probability to learn the entire serial #.

Question: is it provable that the probability to learn the n-bit serial # decreases exponentially with n?
(a) Yes, (b) No.

Furthermore, attempts to learn about c1 ... cn and b1 ... bn alters the original quantum state (lose the money) and the devious behavior may be caught (risk being put in jail).

Topics 11-13: Quantum cryptography in the presence of noise and adversaries

1. Quantum money
2. Quantum bit commitment (M 6.3)
3. Quantum key distribution (NC 12.6, M 6.2)
   - Encryption
   - Classical one-time pad
   - Key distribution problem
   - QKD through a noiseless insecure channel (BB84, E92, and their relation)
   - QKD through noisy insecure channels

Bit commitment

There are 2 parties in bit commitment.

Alice has a bit b that she "commits" to Bob.

Bit commitment

There are 2 parties in bit commitment.

Alice has a bit b that she "commits" to Bob.

Alice wants to keep b secret from Bob until later, when she "reveals" it.

Bit commitment

There are 2 parties in bit commitment.

Alice has a bit b that she "commits" to Bob.

Alice wants to keep b secret from Bob until later, when she "reveals" it.

Bob wants to ensure Alice commits and reveals the same bit.

Bit commitment

There are 2 parties in bit commitment.

Alice has a bit b that she "commits" to Bob.

Alice wants to keep b secret from Bob until later, when she "reveals" it.

Bob wants to ensure Alice commits and reveals the same bit.

The two cryptographic properties of interest are:

1. Binding: Alice cannot commit to one bit, and reveal a different one.

Bit commitment

There are 2 parties in bit commitment.

Alice has a bit b that she "commits" to Bob.

Alice wants to keep b secret from Bob until later, when she "reveals" it.

Bob wants to ensure Alice commits and reveals the same bit.

The two cryptographic properties of interest are:

1. Binding: Alice cannot commit to one bit, and reveal a different one.
2. Concealing: Bob cannot learn the committed bit before it's revealed.

e.g., If Alice has a good lockbox, she can "commit" by writing b on a piece of paper, locking it in the box, and giving the box to Bob without the key. She can reveal the bit later by giving Bob the key.

e.g., If Alice has a good lockbox, she can "commit" by writing b on a piece of paper, locking it in the box, and giving the box to Bob without the key. She can reveal the bit later by giving Bob the key.

In this protocol:

1. binding property comes from Alice not having physical access to the paper after the commit phase

e.g., If Alice has a good lockbox, she can "commit" by writing b on a piece of paper, locking it in the box, and giving the box to Bob without the key. She can reveal the bit later by giving Bob the key.

In this protocol:

1. binding property comes from Alice not having physical access to the paper after the commit phase

2. concealing property comes from assuming that the lockbox cannot be opened without the key (similar to the assumption for the security of cash.)

Why such a strange problem?

Bit commitment is a primitive for many crypto tasks.

Why such a strange problem?

Bit commitment is a primitive for many crypto tasks.

e.g.: remote coin tossing given bit commitment.

In coin tossing, 2 remote parties Alice and Bob want to agree on a random bit.

Why such a strange problem?

Bit commitment is a primitive for many crypto tasks.

e.g.: remote coin tossing given bit commitment.

In coin tossing, 2 remote parties Alice and Bob want to agree on a random bit.

Given secure bit commitment, Alice can commit to a bit b to Bob, afterwards Bob responds to Alice with another bit x of his choice. Alice then reveals b. The resulting coin is $b \oplus x$.

Why such a strange problem?

Bit commitment is a primitive for many crypto tasks.

e.g.: remote coin tossing given bit commitment.

In coin tossing, 2 remote parties Alice and Bob want to agree on a random bit.

Given secure bit commitment, Alice can commit to a bit b to Bob, afterwards Bob responds to Alice with another bit x of his choice. Alice then reveals b. The resulting coin is $b \oplus x$.

Not knowing b, Bob cannot bias the coin with x; "going first" (committing b), Alice can't bias the coin either.

Why such a strange problem?

Bit commitment is a primitive for many crypto tasks.

e.g.: remote coin tossing given bit commitment.

In coin tossing, 2 remote parties Alice and Bob want to agree on a random bit.

Given secure bit commitment, Alice can commit to a bit b to Bob, afterwards Bob responds to Alice with another bit x of his choice. Alice then reveals b. The resulting coin is $b \oplus x$.

Not knowing b, Bob cannot bias the coin with x; "going first" (committing b), Alice can't bias the coin either.

Coin tossing provides trusted randomness for secure distributed computation ... (not just online gambling).

Plausible quantum scheme for bit commitment

Commit phase:

1. Alice picks the bit b she wants to commit to Bob.
2. Alice picks n random bits c1 c2 ... cn.

Plausible quantum scheme for bit commitment

Commit phase:

1. Alice picks the bit b she wants to commit to Bob.
2. Alice picks n random bits c1 c2 ... cn.
3. She sends to Bob: $|c_1\rangle|c_2\rangle\cdots|c_n\rangle$ if b=0

   $H^{\otimes n}\left(|c_1\rangle|c_2\rangle\cdots|c_n\rangle\right)$ if b=1

   (as in Q$ but with b1=b2= ... =bn=b.)

Plausible quantum scheme for bit commitment

Commit phase:

1. Alice picks the bit b she wants to commit to Bob.
2. Alice picks n random bits c1 c2 ... cn.
3. She sends to Bob: $|c_1\rangle|c_2\rangle\cdots|c_n\rangle$ if b=0

   $H^{\otimes n}\left(|c_1\rangle|c_2\rangle\cdots|c_n\rangle\right)$ if b=1

   (as in Q$ but with b1=b2= ... =bn=b.)

4. Bob measures the n qubits, each in a basis randomly chosen from {|0>,|1>} or {|+>,|->}.

Plausible quantum scheme for bit commitment

Commit phase:

1. Alice picks the bit b she wants to commit to Bob.
2. Alice picks n random bits c1 c2 ... cn.
3. She sends to Bob: $|c_1\rangle|c_2\rangle\cdots|c_n\rangle$ if b=0

   $H^{\otimes n}(|c_1\rangle|c_2\rangle\cdots|c_n\rangle)$ if b=1

   (as in Q$ but with b1=b2= ... =bn=b.)
4. Bob measures the n qubits, each in a basis randomly chosen from {|0>,|1>} or {|+>,|->}.

Reveal phase:

1. Alice sends b and c1 c2 ... cn to Bob.

Plausible quantum scheme for bit commitment

Commit phase:

1. Alice picks the bit b she wants to commit to Bob.
2. Alice picks n random bits c1 c2 ... cn.
3. She sends to Bob: $|c_1\rangle |c_2\rangle \cdots |c_n\rangle$ if b=0

   $H^{\otimes n}(|c_1\rangle |c_2\rangle \cdots |c_n\rangle)$ if b=1

   (as in Q$ but with b1=b2= ... =bn=b.)

4. Bob measures the n qubits, each in a basis randomly chosen from {|0>,|1>} or {|+>,|->}.

Reveal phase:

1. Alice sends b and c1 c2 ... cn to Bob.
2. Whether b = 0 or 1, roughly half of the qubits are measured in the "correct" basis. Those outcomes should be consistent with c1 c2 ... cn. Bob accepts only if so.

e.g., n = 10, c1 ... cn = 1100100011

if b=0, state sent to Bob:

$|1\rangle\ |1\rangle\ |0\rangle\ |0\rangle\ |1\rangle\ |0\rangle\ |0\rangle\ |0\rangle\ |1\rangle\ |1\rangle$

e.g., $n = 10$, $c_1 \ldots c_n = 1100100011$

if $b=0$, state sent to Bob:

$$|1\rangle\ |1\rangle\ |0\rangle\ |0\rangle\ |1\rangle\ |0\rangle\ |0\rangle\ |0\rangle\ |1\rangle\ |1\rangle$$

Bob measures in basis:

$$+\ \ +\ \ \times\ \ \times\ \ +\ \ \times\ \ +\ \ +\ \ \times\ \ \times$$

$+ : \{|0\rangle, |1\rangle\}$

$\times : \{|+\rangle, |-\rangle\}$

Question: which can be the 10-bit meas outcome?

(a) 1 0 0 1 1 0 0 0 1 1
(b) 1 1 0 1 1 1 0 0 1 0
(c) 0 1 0 0 1 0 1 0 1 1

e.g., n = 10, c1 ... cn = 1100100011

if b=0, state sent to Bob:

$$|1\rangle\ |1\rangle\ |0\rangle\ |0\rangle\ |1\rangle\ |0\rangle\ |0\rangle\ |0\rangle\ |1\rangle\ |1\rangle$$

Bob measures in basis:

$$+\ \ +\ \ \times\ \ \times\ \ +\ \ \times\ \ +\ \ +\ \ \times\ \ \times$$

$+ : \{|0\rangle, |1\rangle\}$

$\times : \{|+\rangle, |-\rangle\}$

correct bases

wrong bases

(a) 1 0 0 1 1 0 0 0 1 1
(b) 1 1 0 1 1 1 0 0 1 0
(c) 0 1 0 0 1 0 1 0 1 1

e.g., n = 10, c1 ... cn = 1100100011

if b=0, state sent to Bob:

$|1\rangle\ |1\rangle\ |0\rangle\ |0\rangle\ |1\rangle\ |0\rangle\ |0\rangle\ |0\rangle\ |1\rangle\ |1\rangle$

Bob measures in basis:

$+\ \ +\ \ \times\ \ \times\ \ +\ \ \times\ \ +\ \ +\ \ \times\ \ \times$

1 1 1 0 0

bits 1, 2, 5, 7, 8 should be 11100.

$+ : \{|0\rangle, |1\rangle\}$

$\times : \{|+\rangle, |-\rangle\}$

correct bases

wrong bases

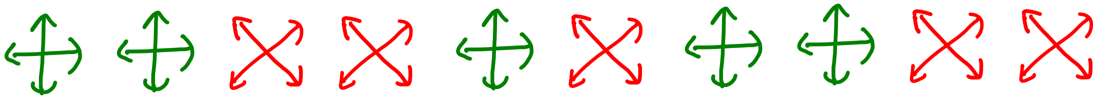
(a) 1 0 0 1 1 0 0 0 1 1
(b) 1 1 0 1 1 1 0 0 1 0
(c) 0 1 0 0 1 0 1 0 1 1

e.g., n = 10, $c1 \ldots cn$ = 1100100011

if b=0, state sent to Bob:

$|1\rangle\ |1\rangle\ |0\rangle\ |0\rangle\ |1\rangle\ |0\rangle\ |0\rangle\ |0\rangle\ |1\rangle\ |1\rangle$

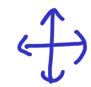
Bob measures in basis:

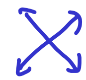


1 1 R R 1 R 0 0 R R

bits 1, 2, 5, 7, 8 should be 11100.

bits 3, 4, 6, 9, 10 are random.

 : $\{|0\rangle, |1\rangle\}$

 : $\{|+\rangle, |-\rangle\}$

correct bases

wrong bases

(a) 1 0 0 1 1 0 0 0 1 1
(b) 1 1 0 1 1 1 0 0 1 0
(c) 0 1 0 0 1 0 1 0 1 1

e.g., n = 10, c1 ... cn = 1100100011

if b=0, state sent to Bob:

$|1\rangle\ |1\rangle\ |0\rangle\ |0\rangle\ |1\rangle\ |0\rangle\ |0\rangle\ |0\rangle\ |1\rangle\ |1\rangle$

Bob measures in basis:

$+\ \ +\ \ \times\ \ \times\ \ +\ \ \times\ \ +\ \ +\ \ \times\ \ \times$

1 1 R R 1 R 0 0 R R

bits 1, 2, 5, 7, 8 should be 11100.

bits 3, 4, 6, 9, 10 are random.

$+ : \{|0\rangle, |1\rangle\}$

$\times : \{|+\rangle, |-\rangle\}$

correct bases

wrong bases

(a) 1 0 0 1 1 0 0 0 1 1
(b) 1 1 0 1 1 1 0 0 1 0
(c) 0 1 0 0 1 0 1 0 1 1

so answer is (b)

e.g., n = 10, c1 ... cn = 1100100011

if b=0, state sent to Bob:

$|1\rangle\ |1\rangle\ |0\rangle\ |0\rangle\ |1\rangle\ |0\rangle\ |0\rangle\ |0\rangle\ |1\rangle\ |1\rangle$

Bob measures in basis:

$+\ \ +\ \ \times\ \ \times\ \ +\ \ \times\ \ +\ \ +\ \ \times\ \ \times$

1 1 R R 1 R 0 0 R R

if b=1, state sent to Bob:

$|-\rangle\ |-\rangle\ |+\rangle\ |+\rangle\ |-\rangle\ |+\rangle\ |+\rangle\ |+\rangle\ |-\rangle\ |-\rangle$

$+ : \{|0\rangle, |1\rangle\}$

$\times : \{|+\rangle, |-\rangle\}$

correct bases

wrong bases

e.g., n = 10, c1 ... cn = 1100100011

if b=0, state sent to Bob:

$|1\rangle \ |1\rangle \ |0\rangle \ |0\rangle \ |1\rangle \ |0\rangle \ |0\rangle \ |0\rangle \ |1\rangle \ |1\rangle$

Bob measures in basis:

$+ \quad + \quad \times \quad \times \quad + \quad \times \quad + \quad + \quad \times \quad \times$

1 1 R R 1 R 0 0 R R

if b=1, state sent to Bob:

$|-\rangle \ |-\rangle \ |+\rangle \ |+\rangle \ |-\rangle \ |+\rangle \ |+\rangle \ |+\rangle \ |-\rangle \ |-\rangle$

Bob measures in basis:

$+ \quad + \quad \times \quad \times \quad + \quad \times \quad + \quad + \quad \times \quad \times$

R R 0 0 R 0 R R 1 1

$+ : \{|0\rangle, |1\rangle\}$

$\times : \{|+\rangle, |-\rangle\}$

correct bases

wrong bases

Intuition for security:

Why Bob cannot learn b?
What is his state for b=0 and b=1?

Intuition for security:

Why Bob cannot learn b?
What is his state for b=0 and b=1?

Both $\left(\frac{I}{2}\right)^{\otimes n}$!

Because $\begin{matrix} \text{wp } \frac{1}{2} : |0\rangle \\ \text{wp } \frac{1}{2} : |1\rangle \end{matrix} \Rightarrow \rho = \frac{I}{2}$ in each qubit for b=0.

Intuition for security:

Why Bob cannot learn b?
What is his state for b=0 and b=1?

Both $\left(\frac{I}{2}\right)^{\otimes n}$!

Because $\begin{array}{l} \text{wp } \frac{1}{2}: |0\rangle \\ \text{wp } \frac{1}{2}: |1\rangle \end{array} \Rightarrow \rho = \frac{I}{2}$ in each qubit for b=0.

But also $\begin{array}{l} \text{wp } \frac{1}{2}: |+\rangle \\ \text{wp } \frac{1}{2}: |-\rangle \end{array} \Rightarrow \rho = \frac{I}{2}$ in each qubit for b=1.

Intuition for security:

Why Bob cannot learn b?
What is his state for b=0 and b=1?

Both $\left(\frac{I}{2}\right)^{\otimes n}$!

Because $\begin{matrix} \text{wp } \frac{1}{2} : |0\rangle \\ \text{wp } \frac{1}{2} : |1\rangle \end{matrix} \Rightarrow \rho = \frac{I}{2}$ in each qubit for b=0.

But also $\begin{matrix} \text{wp } \frac{1}{2} : |+\rangle \\ \text{wp } \frac{1}{2} : |-\rangle \end{matrix} \Rightarrow \rho = \frac{I}{2}$ in each qubit for b=1.

Why can't Alice change her commitment?

Intuition for security:

Why Bob cannot learn b?
What is his state for b=0 and b=1?

Both $\left(\frac{I}{2}\right)^{\otimes n}$!

Because $\begin{array}{l} \text{wp } \frac{1}{2} : |0\rangle \\ \text{wp } \frac{1}{2} : |1\rangle \end{array} \Rightarrow \rho = \frac{I}{2}$ in each qubit for b=0.

But also $\begin{array}{l} \text{wp } \frac{1}{2} : |+\rangle \\ \text{wp } \frac{1}{2} : |-\rangle \end{array} \Rightarrow \rho = \frac{I}{2}$ in each qubit for b=1.

Why can't Alice change her commitment?

The state is already with Bob ... she cannot remotely affect the measurement outcomes.

Intuition for security:

Why Bob cannot learn b?
What is his state for b=0 and b=1?

Both $\left(\frac{I}{2}\right)^{\otimes n}$!

Because $\begin{array}{l} \text{wp } \frac{1}{2} : |0\rangle \\ \text{wp } \frac{1}{2} : |1\rangle \end{array} \Rightarrow \rho = \frac{I}{2}$ in each qubit for b=0.

But also $\begin{array}{l} \text{wp } \frac{1}{2} : |+\rangle \\ \text{wp } \frac{1}{2} : |-\rangle \end{array} \Rightarrow \rho = \frac{I}{2}$ in each qubit for b=1.

Why can't Alice change her commitment?

The state is already with Bob ... she cannot remotely affect the measurement outcomes.

Can we turn the intuition to a rigorous proof ??

Analysis in cryptographic setting:

We can only assume honest (trusted) parties to follow the scheme.

Analysis in cryptographic setting:

We can only assume honest (trusted) parties to follow the scheme.

e.g., the bank is trusted and will follow the scheme,
but no one else is trusted.

Analysis in cryptographic setting:

We can only assume honest (trusted) parties to follow the scheme.

e.g., the bank is trusted and will follow the scheme, but no one else is trusted.

e.g., in bit commitment (and also coin tossing), both parties may cheat, and no one can be trusted.

Analysis in cryptographic setting:

We can only assume honest (trusted) parties to follow the scheme.

e.g., the bank is trusted and will follow the scheme,
but no one else is trusted.

e.g., in bit commitment (and also coin tossing), both
parties may cheat, and no one can be trusted.

What about dishonest parties?
Described by adversarial models.

Adversarial scenarios and models for bit-commitment:

We seeks to protect honest players, not the cheaters.
If both cheat we don't care, if both honest, great.

Adversarial scenarios and models for bit-commitment:

We seeks to protect honest players, not the cheaters.
If both cheat we don't care, if both honest, great.

The interesting cases are:

1. Alice is honest, Bob cheats.
2. Bob is honest, Alice cheats.

1. Alice is honest, Bob cheats.

Alice follows the protocol, and sends the two possible states in the commit phase.

1. Alice is honest, Bob cheats.

Alice follows the protocol, and sends the two possible states in the commit phase.

A dishonest Bob can measure in any way, any time after receiving the state (step 4 or wait until the reveal phase) or not at all! He can accept or reject according to his wimp, without following the scheme.

1. Alice is honest, Bob cheats.

Alice follows the protocol, and sends the two possible states in the commit phase.

A dishonest Bob can measure in any way, any time after receiving the state (step 4 or wait until the reveal phase) or not at all! He can accept or reject according to his wimp, without following the scheme.

Qn: Can Bob learn about b before the reveal phase?

1. Alice is honest, Bob cheats.

Alice follows the protocol, and sends the two possible states in the commit phase.

A dishonest Bob can measure in any way, any time after receiving the state (step 4 or wait until the reveal phase) or not at all! He can accept or reject according to his wimp, without following the scheme.

Qn: Can Bob learn about b before the reveal phase?

Concealing property of proposed scheme:

Bob cannot learn b before the reveal phase because his state for both b=0 and b=1 cases is $(I/2)^{\otimes n}$.

2. Bob is honest, Alice cheats.

Bob follows the protocol and measures in random bases in step 4 of commit phase, and accept/reject as instructed in the reveal phase.

2. Bob is honest, Alice cheats.

Bob follows the protocol and measures in random bases in step 4 of commit phase, and accept/reject as instructed in the reveal phase.

In the commit phase, Alice can send any n qubits to Bob. In the reveal phase, Alice can send any n+1 bits.

2. Bob is honest, Alice cheats.

Bob follows the protocol and measures in random bases in step 4 of commit phase, and accept/reject as instructed in the reveal phase.

In the commit phase, Alice can send any n qubits to Bob. In the reveal phase, Alice can send any n+1 bits.

Qn: Will Bob reject ?

2. Bob is honest, Alice cheats.

Bob follows the protocol and measures in random bases in step 4 of commit phase, and accept/reject as instructed in the reveal phase.

In the commit phase, Alice can send any n qubits to Bob. In the reveal phase, Alice can send any n+1 bits.

Qn: Will Bob reject ?

Binding property: once sent, Alice cannot changed the state Bob receives and cannot affect his measurements, nor the outcomes ...

2. Bob is honest, Alice cheats.

Bob follows the protocol and measures in random bases in step 4 of commit phase, and accept/reject as instructed in the reveal phase.

In the commit phase, Alice can send any n qubits to Bob. In the reveal phase, Alice can send any n+1 bits.

Qn: Will Bob reject ?

Binding property: once sent, Alice cannot changed the state Bob receives and cannot affect his measurements, nor the outcomes ...

BUT Bob accepts/rejects based on his meas outcomes AND Alice's message in the reveal phase (b c1 ... cn). So, it depends on THEIR CORRELATION!

2. Bob is honest, Alice cheats.

Bob follows the protocol and measures in random bases in step 4 of commit phase, and accept/reject as instructed in the reveal phase.

In the commit phase, Alice can send any n qubits to Bob. In the reveal phase, Alice can send any n+1 bits.

Qn: Will Bob reject ?

Binding property: once sent, Alice cannot changed the state Bob receives and cannot affect his measurements, nor the outcomes ...

BUT Bob accepts/rejects based on his meas outcomes AND Alice's message in the reveal phase (b c1 ... cn). So, it depends on THEIR CORRELATION!

Recall entanglement can create unexpected quantum correlations, e.g., in the GHZ game!

Mayers, Lo, Chau 96

There is no secure bit commitment scheme in the quantum setting.

Mayers, Lo, Chau 96

There is no secure bit commitment scheme in the quantum setting.

This is an example of a no-go theorem. It is a very strong statement since it does not only say that certain scheme is insecure. It says no matter how hard researchers try, all such schemes are insecure.!

Mayers, Lo, Chau 96

There is no secure bit commitment scheme in the quantum setting.

This is an example of a no-go theorem. It is a very strong statement since it does not only say that certain scheme is insecure. It says no matter how hard researchers try, all such schemes are insecure.!

E.g., What goes wrong with the proposed scheme --
The "analysis" has a hidden assumption, that Alice is sending Bob a pure state based on c and b1 ... bn. She can instead send n qubits that are entangled with some system in her lab, and create correlations that let her cheat !

Mayers, Lo, Chau 96

There is no secure bit commitment scheme in the quantum setting.

Proof: the most general thing Alice can do is to prepare some $|\psi_0\rangle$ if b=0, and some $|\psi_1\rangle$ if b=1.

Mayers, Lo, Chau 96

There is no secure bit commitment scheme in the quantum setting.

Proof: the most general thing Alice can do is to prepare some $|\psi_0\rangle$ if b=0, and some $|\psi_1\rangle$ if b=1.

$|\psi_0\rangle$ lives in the systems A0 B where B is 2^n dim.

$|\psi_1\rangle$ lives in the systems A1 B where B is 2^n dim.

Mayers, Lo, Chau 96

There is no secure bit commitment scheme in the quantum setting.

Proof: the most general thing Alice can do is to prepare some $|\psi_0\rangle$ if b=0, and some $|\psi_1\rangle$ if b=1.

$|\psi_0\rangle$ lives in the systems A0 B where B is 2^n dim.

$|\psi_1\rangle$ lives in the systems A1 B where B is 2^n dim.

If the scheme is concealing, the state received by Bob is the same whether b=0 or 1:

$$\mathrm{Tr}_{A_0} |\psi_0\rangle\langle\psi_0| = \mathrm{Tr}_{A_1} |\psi_1\rangle\langle\psi_1| = \rho_B$$

Mayers, Lo, Chau 96

There is no secure bit commitment scheme in the quantum setting.

Proof: the most general thing Alice can do is to prepare some $|\psi_0\rangle$ if b=0, and some $|\psi_1\rangle$ if b=1.

$|\psi_0\rangle$ lives in the systems A0 B where B is 2^n dim.

$|\psi_1\rangle$ lives in the systems A1 B where B is 2^n dim.

If the scheme is concealing, the state received by Bob is the same whether b=0 or 1:

$$\mathrm{Tr}_{A_0} |\psi_0\rangle\langle\psi_0| = \mathrm{Tr}_{A_1} |\psi_1\rangle\langle\psi_1| = \rho_B$$

So, $|\psi_0\rangle, |\psi_1\rangle$ are purifications of the same state ρ_B

Mayers, Lo, Chau 96

There is no secure bit commitment scheme in the quantum setting.

Proof: the most general thing Alice can do is to prepare some $|\psi_0\rangle$ if b=0, and some $|\psi_1\rangle$ if b=1.

$|\psi_0\rangle$ lives in the systems A0 B where B is 2^n dim.

$|\psi_1\rangle$ lives in the systems A1 B where B is 2^n dim.

If the scheme is concealing, the state received by Bob is the same whether b=0 or 1:

$$\mathrm{Tr}_{A_0} |\psi_0\rangle\langle\psi_0| = \mathrm{Tr}_{A_1} |\psi_1\rangle\langle\psi_1| = \rho_B$$

So, $|\psi_0\rangle, |\psi_1\rangle$ are purifications of the same state ρ_B

But 2 purifications of the same density matrix are related by an isometry between the purifying systems:

$$\therefore \; |\psi_0\rangle = U \otimes I \, |\psi_1\rangle$$

$\therefore |\psi_0\rangle = U \otimes I \, |\psi_1\rangle$

But it means a cheating Alice can prepare $|\psi_1\rangle$ during during the commit phase, and decide b ONLY at the reveal phase: if b=1, does nothing, if b=0, apples U to A1 to transform the global state to $|\psi_0\rangle$.

$\therefore\ |\psi_0\rangle = U \otimes I\ |\psi_1\rangle$

But it means a cheating Alice can prepare $|\psi_1\rangle$ during during the commit phase, and decide b ONLY at the reveal phase: if b=1, does nothing, if b=0, apples U to A1 to transform the global state to $|\psi_0\rangle$.

Either case, Bob accepts. Concealing => not binding.

$\therefore\ |\psi_0\rangle = U \otimes I\, |\psi_1\rangle$

But it means a cheating Alice can prepare $|\psi_1\rangle$ during during the commit phase, and decide b ONLY at the reveal phase: if b=1, does nothing, if b=0, apples U to A1 to transform the global state to $|\psi_0\rangle$.

Either case, Bob accepts. Concealing => not binding.

* Bob's reduced state and outcomes are unchanged by Alice's cheating (no-signalling) but Alice's message in the reveal phase is correlated with Bob's outcome such that Bob always accepts.

E.g. How to cheat in the proposed scheme:

Original:

3. She sends to Bob: $|c_1\rangle|c_2\rangle\cdots|c_n\rangle$ if b=0

$H^{\otimes n}(|c_1\rangle|c_2\rangle\cdots|c_n\rangle)$ if b=1

E.g. How to cheat in the proposed scheme:

Original:

3. She sends to Bob: $|c_1\rangle |c_2\rangle \cdots |c_n\rangle$ if b=0

$H^{\otimes n}(|c_1\rangle |c_2\rangle \cdots |c_n\rangle)$ if b=1

A cheating Alice does not commit to any b nor send any of the above states. Instead, she prepares n copies of Bell pairs, and sends one qubit of each pair to Bob, resulting in the joint state:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{A_1B_1} \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{A_2B_2} \otimes \cdots \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{A_nB_n}$$

E.g. How to cheat in the proposed scheme:

Original:

3. She sends to Bob: $|c_1\rangle|c_2\rangle\cdots|c_n\rangle$ if b=0

$H^{\otimes n}(|c_1\rangle|c_2\rangle\cdots|c_n\rangle)$ if b=1

A cheating Alice does not commit to any b nor send any of the above states. Instead, she prepares n copies of Bell pairs, and sends one qubit of each pair to Bob, resulting in the joint state:

$$\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{A_1B_1} \otimes \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{A_2B_2} \otimes \cdots \otimes \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{A_nB_n}$$

Bob follows the protocol, measures B1 B2 ... Bn. But since operations on A1 ... An commute with those on B1 ... Bn, we can analyse the situation as if Alice's operations in the reveal phase happen first !

At the reveal phase, Alice picks b.

If b=0, she measures each of A1 A2 ... An along the {|0>,|1>} basis, the random outcomes c1 c2 ... cn & b=0 are sent to Bob. The postmeasurement state on B1 B2 ... Bn is $|c_1\rangle |c_2\rangle \cdots |c_n\rangle$.

At the reveal phase, Alice picks b.

If b=0, she measures each of A1 A2 ... An along the {|0>,|1>} basis, the random outcomes c1 c2 ... cn & b=0 are sent to Bob. The postmeasurement state on B1 B2 ... Bn is $|c_1\rangle|c_2\rangle \cdots |c_n\rangle$.

Bob's measurements on B1 B2 ... Bn have outcomes as if Alice had committed to b=0 at the commit phase.

At the reveal phase, Alice picks b.

If b=0, she measures each of A1 A2 ... An along the {|0>,|1>} basis, the random outcomes c1 c2 ... cn & b=0 are sent to Bob. The postmeasurement state on B1 B2 ... Bn is $|c_1\rangle|c_2\rangle\cdots|c_n\rangle$.

Bob's measurements on B1 B2 ... Bn have outcomes as if Alice had committed to b=0 at the commit phase.

If b=1, Alice measures each of A1 A2 ... An along the {|+>,|->} basis, sends c1 ... cn & b=1 to Bob. Ex:

$$\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right) = \frac{1}{\sqrt{2}}\left(|++\rangle+|--\rangle\right)$$

Postmeas state in B1 B2 .. Bn is: $H^{\otimes n}\left(|c_1\rangle|c_2\rangle\cdots|c_n\rangle\right)$

At the reveal phase, Alice picks b.

If b=0, she measures each of A1 A2 ... An along the {|0>,|1>} basis, the random outcomes c1 c2 ... cn & b=0 are sent to Bob. The postmeasurement state on B1 B2 ... Bn is $|c_1\rangle|c_2\rangle\cdots|c_n\rangle$.

Bob's measurements on B1 B2 ... Bn have outcomes as if Alice had committed to b=0 at the commit phase.

If b=1, Alice measures each of A1 A2 ... An along the {|+>,|->} basis, sends c1 ... cn & b=1 to Bob. Ex:

$$\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right) = \frac{1}{\sqrt{2}}\left(|{+}{+}\rangle+|{-}{-}\rangle\right)$$

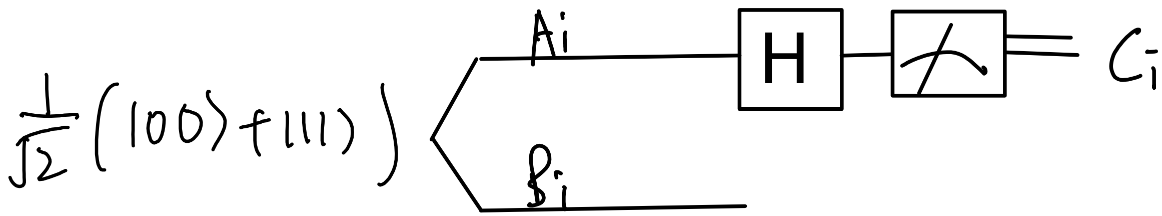
Postmeas state in B1 B2 .. Bn is: $H^{\otimes n}\left(|c_1\rangle|c_2\rangle\cdots|c_n\rangle\right)$

Bob sees outcomes as if Alice had commited to b=1.

Bob always accepts ....

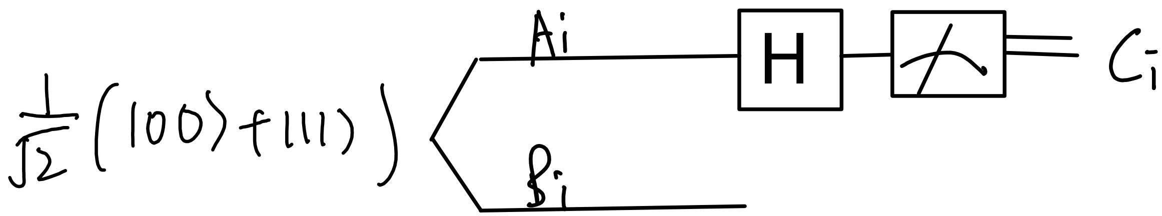
Alternative derivation of the postmeasurement state:

Measurement along {|+>,|->} =
Hadamard followed by measurement along {|0>,|1>}

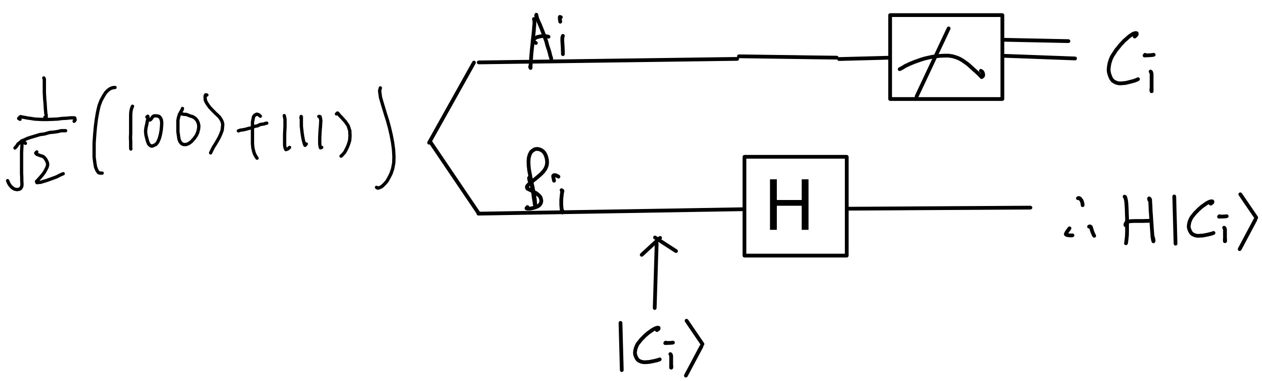


Alternative derivation of the postmeasurement state:

Measurement along {|+>,|->} =
Hadamard followed by measurement along {|0>,|1>}



Using the transpose trick (A1), if the transpose of H
is applied to Bi, we get the same state as above:



Lesson:

Entanglement is really useful, to everyone.

If it helps you teleport, superdense code etc, it can also help the adversary. We must consider the most general attack allowed by QM if there is no reason to restrict the adversary.

Lesson:

Entanglement is really useful, to everyone.

If it helps you teleport, superdense code etc, it can also help the adversary. We must consider the most general attack allowed by QM if there is no reason to restrict the adversary.

Lose ends:

Will a multi-message commit phase help? No ...
Focus on Bob's state for b=0/1 at the end of the commit phase.

Lesson:

Entanglement is really useful, to everyone.

If it helps you teleport, superdense code etc, it can also help the adversary. We must consider the most general attack allowed by QM if there is no reason to restrict the adversary.

Lose ends:

Will a multi-message commit phase help? No ...
Focus on Bob's state for b=0/1 at the end of the commit phase.

Researchers subsequently add constraints BEYOND QM, e.g., special relativity (that one cannot signal faster than the speed of light) or change the game ...