1 Readings

Benenti, Casati, and Strini:

Superdense Coding Ch.4.4

Quantum Cryptography Ch. 4.1, 4.3

2 Superdense Coding

Super dense coding is the less popular sibling of teleportation. It can actually be viewed as the process in reverse. The idea is to transmit two classical bits of information by only sending one quantum bit. The process starts out with an EPR pair that is shared between the sender (Alice) and receiver (Bob).

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

The first qubit is Alice's, the second is Bob's.

Alice wants to send a two bit message to Bob, e.g., 00, 01, 10, or 11. She first performs a single qubit operation on her qubit which transforms the EPR pair according to which message she wants to send:

- for a message **00**: Alice applies I (i.e., does nothing)
- for a message **01**: Alice applies X
- for a message **10**: Alice applies Z
- for a message **11**: Alice applies iY (i.e. both X and Z)

This transforms the EPR pair $|\phi^+\rangle$ into the four Bell (EPR) states $|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle$, and $|\psi^-\rangle$, respectively:

- **00**: $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \longrightarrow \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$
- **01**: $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \longrightarrow \frac{1}{\sqrt{2}}\left(|10\rangle + |01\rangle\right) = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$
- **10**: $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \longrightarrow \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \end{bmatrix}$

- **11**: $i\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right) \longrightarrow \frac{1}{\sqrt{2}}\left(|01\rangle-|10\rangle\right)=\frac{1}{\sqrt{2}}\begin{bmatrix} 0 \\ 1 \\ -1 \\ 0 \end{bmatrix}$

The key to super-dense coding is that these four Bell states are orthonormal and are hence distinguishable by a quantum measurement, in this case a two-qubit measurement made by Bob. This measurement can be performed directly in the Bell basis. Alternatively, Bob can first run the quantum circuit for forming Bell states from computational basis states backwards, and then measure in the computational basis to get either 00, 01, 10, or 11.

Examining this process in more detail:

$|\psi_{00}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)=\frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle+|1\rangle|1\rangle\right)$

apply *CNot* gives us: $\frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle+|1\rangle|0\rangle\right)$

apply H gives us: $\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\left(\left(|0\rangle+|1\rangle\right)|0\rangle+\left(|0\rangle-|1\rangle\right)|0\rangle\right)=$

$\frac{1}{2}\left(|00\rangle+|10\rangle+|00\rangle-|10\rangle\right)=|00\rangle$

Bob now measures both qubits to get Alice's message 00

$|\psi_{01}\rangle = \frac{1}{\sqrt{2}}\left(|10\rangle+|01\rangle\right)=\frac{1}{\sqrt{2}}\left(|1\rangle|0\rangle+|0\rangle|1\rangle\right)$

apply *CNot* gives us: $\frac{1}{\sqrt{2}}\left(|1\rangle|1\rangle+|0\rangle|1\rangle\right)$

apply H gives us: $\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\left(\left(|0\rangle-|1\rangle\right)|1\rangle+\left(|0\rangle+|1\rangle\right)|1\rangle\right)=$

$\frac{1}{2}\left(|01\rangle-|11\rangle+|01\rangle+|11\rangle\right)=|01\rangle$

Bob now measures both qubits to get Alice's message 01

$|\psi_{10}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle-|11\rangle\right)=\frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle-|1\rangle|1\rangle\right)$

apply *CNot* gives us: $\frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle-|1\rangle|0\rangle\right)$

apply H gives us: $\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\left(\left(|0\rangle+|1\rangle\right)|0\rangle+\left(|1\rangle-|0\rangle\right)|0\rangle\right)=$

$\frac{1}{2}\left(|00\rangle+|10\rangle+|10\rangle-|00\rangle\right)=|10\rangle$

Bob now measures both qubits to get Alice's message 10

Check the last one, $|\psi_{11}\rangle \longrightarrow 11$, yourself.

3 Quantum Cryptography

Cryptography is the science(or art, depending on your perspective) of secret communication. Successful cryptography should also be able to detect eavesdropping. Quantum cryptography enables two parties, Alice (the sender) and Bob (the receiver), to send a secret message and also to detect whether an eavesdropper (Eve) is trying to listen in. This remarkable feature is due to the impossibility of copying an unknown quantum state (no-cloning theorem). We shall first summarize the classical protocol for a secure code (one-time key pad), then describe two quantum protocols for secure key distribution.

3.1 One-time key pad

- write the plaintext message as a sequence of 0's and 1's (not random)

  $p_1 p_2, \ldots p_n$

- take a secret key shared only between sender and receiver, consisting of a random binary sequence of same length n as the binary message

  $k_1, k_2, \ldots k_n$

- the cypher text to be transmitted over an insecure channel is obtained as the bitwise sum modulo 2 of the plaintext and keytext, $c_i = p_i \oplus k_i$

The receiver can then invert the cypher text to reconstruct the plaintext if he/she possesses the secret key k_i. This classical protocol is provably secure if the key is truly secret, the key is used only once (since the plaintext is not random and will have redundancies that will enable decoding by clever pattern recognition if the key is used multiple times), and the key is truly random. In order to guarantee security, the two parties need therefore to

i) be able to generate long random binary strings, one for each message

ii) to be able to share the secret keys without other parties gaining access.

Neither of these requirements are easy in practice.

3.2 Generating a quantum key from EPR correlations

Suppose Alice produces pairs of entangled qubits $|\psi_{ab}\rangle = \frac{1}{\sqrt{2}}(|0_a 1_b\rangle - |1_a 0_b\rangle)$ and sends the second qubit from each pair to Bob through a public quantum channel. If both Alice and Bob then make measurements in the computational basis, then Alice will get a random string of 0's and 1's and Bob will obtain the complementary string, i.e., whenever Alice has a 0, Bob has a 1. Then Bob just needs to take the complement of his measurement to obtain the same string as Alice and they have a shared key. Now how secret is this key? Clearly if no one disturbs the qubits being sent from Alice to Bob, the key is secure. The key is random since the projective measurements necessarily produce random results, and can be made arbitrarily long provided Alice has a reliable source of EPR pairs. But is it secure against an eavesdropper? Supposing Eve wants to listen in. She knows the protocol being used by Alice and Bob (this is public) and can thus intercept the second qubit of each pair and measure it in the computational basis before Bob. She can thus get Bob's information and then send off a new qubit to Bob in the same state she obtained from measurement. Eve has thus broken the code and Bob (and Alice) are not aware of this.

You may guess from our earlier analysis of the EPR correlations and Bell inequality, that what Alice and Bob need to do to protect their key against Eve is to make measurements in two bases, instead of one. This is the basis of the protocol proposed by Ekert, PRL 67, p. 661 (1991). Here is a simplified version (Ekert used three bases for measurement, rather than two).

Alice and Bob choose randomly (and privately) to measure their qubits in either 0/1 or +/- bases. For example, if Alice measures in the +/- basis, she finds + with probability 1/2, and - with probability 1/2.

Recall $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

If Alice measures +, then Bob will automatically have $|-\rangle$ since the EPR pairs are entangled and perfectly anticorrelated. Now Eve intercepts Bob's qubit. She knows the protocol but now has to guess which basis to measure in, since Alice's choice of basis for each measurement is privately determined. Suppose Eve measures in the 0/1 basis, and gets a 0. She can send on a new $|0\rangle$ qubit to Bob after recording this, or in fact any state. Suppose she sends on $|0\rangle$. Bob now receives $|0\rangle$ rather than the $|-\rangle$ which he would have received directly from Alice. If Bob had privately decided to measure this qubit in the +/- basis he will now obtain + with probability 1/2 and - with probability 1/2, instead of - with probability 1 as he would have done if Eve had not intercepted his qubit. So on some occasions he will have an erroneous measurement. Eve's interception has changed the state for Bob, removing the entanglement of this qubit with Alice's qubit.

Alice and Bob can now detect Eve's interception by measuring the quantum correlations between some representative fraction of their qubits and seeing whether these satisfy the Bell inequality. If yes, they conclude Eve is absent and the key secure, if no, they know that Eve is listening in and can decide whether or not to use the key. Here is the full protocol.

- Transmission of long string of EPR pairs $|\psi^-\rangle$ to Alice and Bob (or Alice sends second qubit of a pair she generates to Bob)

  Alice measures randomly in 0/1 or +/- basis

  Bob measures randomly in 0/1 or +/- basis

  Eve does her best, so measures also randomly in 0/1 or +/- basis

- After n EPR pairs have been processed, Alice and Bob broadcast their measurement bases (but not the results of the measurements)

  They compare their bases and divide the n sets of measurements into 3 groups:

  i) same bases used by Alice and Bob

  ii) different bases used by Alice and Bob

  iii) dud measurement, either Alice or Bob failed to record a qubit (loss)

  Group iii) is rejected.

- Alice and Bob share, i.e., reveal publicly, the measurement results from group ii) and some of those from group i). They use these to evaluate the Bell correlation $|<g>| = |<AB> + <A'B> + <AB'> - <A'B'>|$. If $|<g>| > 2$ then all pairs are entangled, there is no Eve and the key will be secret. If $|<g>| < 2$ they know that the entanglement is removed, only classical correlations remain and Eve is listening in.

- If the entanglement signifies no Eve, Alice and Bob then take the remainder of their measurements from group i) and use these anticorrelated measurements to construct the secret key as before.

3.3 Quantum Key Distribution with BB84

The BB84 protocol (Bennett and Brassard, Proc. of IEEE Int. Conf. on Computers, Systems and Signal Processing, p. 175, IEE, Hew York, 1984) uses strings of single qubits produced in two non-orthogonal bases. It relies explicitly on the imperfect distinguishability of non-orthogonal states (see no-cloning theorem) to guarantee security.

- Alice sends a single qubit to Bob in either the 0/1 or +/- basis. Thus Alice is randomly encoding into one of two non-orthogonal bases. On average she sends half in each basis.

- Bob decides at random whether to measure in the 0/1 or +/- basis. On average he measures half in each basis.

- Eve?? Eve cannot copy the transmitted photon, and so also cannot distinguish which basis it is in without disturbing it. Thus it is impossible for her to make some unitary operation resulting in

$$\begin{aligned} \left|\psi\right\rangle\left|u\right\rangle &\to \left|\psi\right\rangle\left|v\right\rangle \\ \left|\phi\right\rangle\left|u\right\rangle &\to \left|\phi\right\rangle\left|v'\right\rangle \end{aligned}$$

  with $\left|v\right\rangle \neq \left|v'\right\rangle$ so that she can measure the ancillas $\left|v\right\rangle$ and $\left|v'\right\rangle$ and thereby distinguish whether the initial state was $\left|\psi\right\rangle$ or $\left|\phi\right\rangle$, since inner products are preserved under unitaries. Hence $\left\langle v\right|\left.v'\right\rangle\left\langle\psi\right|\left.\phi\right\rangle = \left\langle u\right|\left.u\right\rangle\left\langle\psi\right|\left.\phi\right\rangle = \left\langle\psi\right|\left.\phi\right\rangle$ which implies that $\left\langle v\right|\left.v'\right\rangle = 1$, i.e., $\left|v\right\rangle$ and $\left|v'\right\rangle$ are the same state. So Eve has to make a measurement. But she cannot measure in both bases simultaneously...

- Alice and Bob broadcast which basis they used for each qubit.

- Alice and Bob each delete all instances where they used different bases. This leaves them with a raw key.

- Alice and Bob announce part of the raw key publicly and use this to obtain the error rate due to eavesdropping by Eve. They can do this just by comparing the measurements of Bob with the qubit sent by Alice.

The security of this protocol relies on the impossibility of cloning an unknown quantum state (Alice's sent qubit), the fact that measurements by Eve will change the qubit state so that Eve's actions may be detected, and the generation of a random choice of bases by Alice (think about how to ensure this). In practice some additional steps are need to ensure an acceptable security. See Benenti et al., or Neilsen and Chuang. The BB84 and related protocols are used experimentally with photon polarization as the qubit states. See handout. Commercially available prototypes have also been recently developed, see http://magiq.nowwireless.com/.

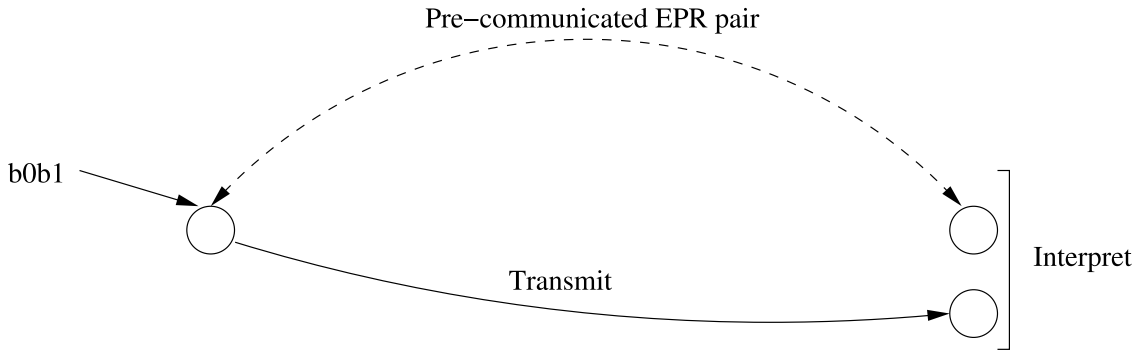

Figure 1: Superdense coding works by first pre-communicating an EPR pair between sender (Alice, on left) and receiver (Bob, on right). Alice first manipulates her half of this EPR pair (a single qubit) according to which two classical bit message she wishes to transmit, and then sends her qubit to Bob. Bob then makes some two qubit manipulations and finally measures both bits to obtain the two bits of classical information.

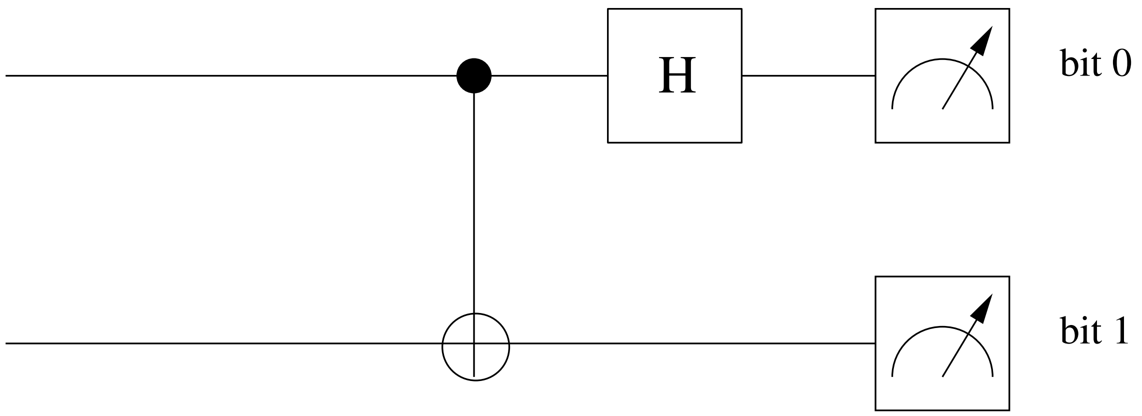

Figure 2: To obtain the two bits of classical information this circuit is implemented by Bob on the two qubits, one of which has been sent by Alice. Bob's circuit is equivalent to making a measurement in the Bell-basis.