Topics in Quantum Information | **U. Waterloo CO 781, Fall 2006**
Lecturer: Ashwin Nayak | **Scribe: Abhinav Bahadur**
Security of BB84 | **November 6,8, 2006**

DRAFT

In this lecture we show the security of the BB84 Quantum Key Distribution Protocol. The proof is done by modifying the Lo Chau protocol to the BB84 protocol and appealing to the security of the Lo Chau Protocol

Recall the Lo Chau kind of protocol where the operations of Alice are
1.Measure check bits in the computatoinal basis.
2.Measure the syndrome in the code qubits.
3.Decode the residual state to get the key k.

Now these operations can be performed immediately after EPR pairs are prepared. So effectively

1. Alice may simply choose a uniform random state $|0\rangle$ and $|1\rangle$ and instead of preparing EPR pairs for their check bits

Recall that a quantum CSS code on n qubits is given by 2 binary code C_1 and C_2 such that C_2 is a subspace of C_1
Fact: The $n-$ qubit Hilbert space decomposes as
$(\mathbb{C}^2)^{\otimes n} = \oplus_{x \in Z_2^n/C_1, z \in Z_2^n/C_2^\perp} Q_{x,z}$
where $Q_{x,z}$ is the subspace spanned by $\{|\xi_{x,z}(v)\rangle\}_{v_2 \in C_1/C_2}$ and $|\xi_{x,z}(v)\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} (-1)^{w.z} |w + v + x\rangle$
Now these are orthogonal for x emerging from distinct cosets of C_1 on Z_2^n and for z from distinct cosets of $C_2^\perp$ in Z_2^n.
We have the dimension of $Q_{x,z}$ equal to $\frac{|C_1|}{|C_2|}$ and the number of distinct cosets of C_1 equal to $\frac{2^n}{|C_1|}$ and the number of cosets of $C_2^\perp$ equal to $\frac{2^n}{|C_2^\perp|} = |C_2|$. And for a fixed x, v we have
$\langle \xi_{x,z}(v) | \xi_{x,z}(v) \rangle = \frac{1}{|C_2|} \sum_{w_1, w_2 \in C_2} (-1)^{w_1 z_1 + w_2 z_2} \langle w_1 + v + x | w_2 + v + x \rangle$. The inner products are non-zero when $w_1 = w_2$, which gives $\langle \xi_{x,z}(v) | \xi_{x,z}(v) \rangle = \frac{1}{|C_2|} \sum_{w \in C_2} (-1)^{w z_1 + w z_2} = 1$ if $z_1 + z_2 \in C_2^\perp$ and 0 otherwise.

2.Since x, z, k are uniformly distributed over $Z_2^n/C_1, z$,$Z_2^n/C_2^\perp$ and C_1/C_2, Alice may pick these uniformly at random from the subspaces and encode k in the subspace $Q_{x,z}$ to generate Bob's code qubits.

Note that since $|\xi_{x_1,z_1}(v)\rangle = |\xi_{x_2,z_2}(v)\rangle$ IFF $x_1 + x_2 \in C_1$ and $z_1 + z_2 \in C_2^\perp$ Alice may pick x, z uniformly at random from Z_2^n.

This leads us to protocol 2, the CSS code protocol due to Shor Preskill.

1. A creates n random check bits and m key bits k (where $m = \dim(C_1) - \dim(C_2)$), and a random $2n$ bit string k.
2. A chooses x, z, which are n bit strings uniformly at random.
3. A encodes k in the CSS code $Q_{x,z}$.
4. A chooses n out of $2n$ positions to be the check qubits and the places the check and code qubits appropriately.
5. Applies a H on every qubit given by $b_i = 1$.
6. A sends all qubits to B, who acknowledges.
7. Alice announces b, the positions and values of the check bits x, z.
8. B applies H on qubits specified by the bit string b.

9. B measures them in the computational basis and they abort if there are too many errors.
10. Bob decodes code qubits to $Q_{x,z}$ and gets the key k.

We show a relation between the CSS codes protocol(2nd protocol in paper) to the BB84 protocol(3rd in paper). The steps that we need to recall are the following
Alice does the following 1. Picks n random test bits and m random key bits.
2. Picks n random bit strings x, z for the shifted CSS codes and encodes k in $Q_{k,z}$

After the test phase passes Bob decodes the key from its encoding in $Q_{x,z}$ i.e he performs the bit and phase error correction. Bob needs x for bit error and z for phase error correction.

Now we observe that phase correction is unnecessary in the Lo-Chau protocol and hence the CSS codes protocol. Hence Alice need not send the bit string z which is required for phase error correction.

Now we have the following
$|k\rangle \longrightarrow \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} (-1)^{w.z} |v_k + w + x\rangle = |\xi_{x,z}(v)\rangle$.
Now z is now available to B his state is described by a mixed density matrix ρ_B given by
$\frac{1}{2^n} \sum_z |\xi_{x,z}(v)\rangle\langle\xi_{x,z}(v)|$
which is equal to $\frac{1}{2^n|C_2|} \sum_z \sum_{w_1,w_2 \in C_2} (-1)^{(w_1+w_2).z} |v_k + w_1 + x\rangle\langle v_k + w_2 + x|$.
We need that $w_1 = w_2$ which gives
$\rho_B = \frac{1}{|C_2|} \sum_{w \in C_2} |v_k + w + x\rangle\langle v_k + w + x|$.
From this expression we can conclude that instead of encoding in the CSS code she may have equivalently encoded it as a mixture of a classical code words in a coset or C_2 in Z_2^n. Hence Alice can do the following
1 Pick up x uniformly at random from Z_2^n
2. Pick a random $w \in C_2$ and send $|v_k + w + x\rangle$.

When these modifications are made Bob changes his error correction and decodong step as
1. Receive x from Alice and correct errors according to the coset $x + C_1$ i.e his string looks like $v_k + w + x + e_b$ which is sometimes called the sifted key where e_b is the error introduced by the eavesdropping channel. He adds the string x to the sifted key , and gets $v_k + w + e_b$. Since $v_k + w \in C_1$ he corrects bit errors e_b.

Now he can compute the coset representative v_k of this string $v_k + w$ in C_1.
Including these changes in CSS code protocol we get the BB84 protocol which we now write down.

1. Alice picks $2n$ random bits (n test bits and n code bits). Note here that $v_k + x + w$ is uniformly at random since k, w, x were chosen at random.(x is uniformly at random). So we can pick a value for this and then pick w and v_k from the appropriate conditional distributions.
2. picks a $2n$ bit random string b and rotates all the bits in position i by H where $b_i = 1$.
3. Send these to Bob
4.Bob acknowledges receipt
5.Alice announces b.

6.B undoes the H operation on positions i where $b_i = 1$. Announces the positions of check bits, both measure these in computational basis. Abort if there are too many positions in which they disagree.
(error correction and privacy amplification)
7-10. At this time they both share the sifted key. (Bob's key may have errors due to eavesdropping). So they both extract the key as before

Now we observe that at step 4 Bob has to store the qubits which can be eliminated. This is done as follows by modifying the number of selections in the previous protocol
1.A picks up $(4 + \delta)n$ random bits

2,3.A picks up $(4+\delta)n$ bit string b.
4. Bob acknowledges , after measuring each qubit in a random basis , computational basis or the Hadamard basis.
5.(no change)
6.B discards all qubits measured in the wrong basis. Now with high probability they both have $2n$ bits and continue as before.

Final Remarks
1. There are code pairs C_1, C_2 required for CSS coding with rate that go by $1 - 2H_2(2\delta)$ where H is the entropy and C_1, C_2 can correct δn bit and flip errors. So starting with $(4+\delta)n$ qubits sent in 1^{st} step we get $(1 - 2H_2(2\delta))$ bits of key
2. Security of the proof relies on
(a) Ability to prepare single qubit states. Laser which is used to prepare quantum states have a property that emit multible qubits that are entangled and the eavesdropper may split the beam and keep some infomation (b) Measurement appratus accurate
However we can generalize this proof to handle some of these imperfections.