Quantum cryptography

Lecture Notes for Quantum Computing

Lecturer: Dorit Aharonov
Scribe: Eran Rom

July 2001

Abstract

We start with introducing the bit commitment protocol and show a naive quantum implementation of it, which turns out to be insecure. Then, we show that there is no secure quantum implementation of bit commitment protocol, in general. To do that we will introduce and prove the Schmidt decomposition theorem. We will also show that a non-ideal bit commitment protocol is also impossible to implement. Unlike the bit commitment protocol, where the quantum model does not give any advantage over the classic model, there is a secure public key distribution protocol, which make no computational assumptions. We will show the protocol and explain its security, which is based on random sampling and the entanglement purification protocol.

1 Bit Commitment

Bit commitment is a basic building block for many cryptography protocols, such as zero knowledge proofs. Bit commitment is a protocol between two parties (typically, Alice and Bob). The protocol has two stages: the commit stage and the reveal stage. In the commit stage Alice chooses a bit and makes a commitment about her choice to Bob. The commitment is done in such a way that Bob has no information about her choice. In the reveal stage Alice reveals her choice to Bob. The protocol assures that Alice cannot reveal, a choice different from the one she committed on. Using the bit commitment protocol we can build a coin flipping protocol, a basic need for any Internet based gambling game. Alice and Bob choose a bit and make a commitment to each other. Once the commitment of both sides is done, they reveal their choices. At the end, each of them "xors" his own choice with the other side's choice to have a shared "flipped coin". Still there is a theoretical obstacle preventing from opening a gambling ".com". The bit commitment protocol can be done classically, only under assumptions of the hardness of some computational problems. Even worse, the basic assumption in quantum mechanics, where looking at something changes it, an assumption which seems to help in this case, doesn't. We will prove that a secured bit commitment protocol is impossible in the quantum model.

1.1 A naive protocol for bit commitment

Although we know by now that such a protocol does not exist, we will start be showing a naive protocol for bit commitment, which fails to be secure.

The commitment stage: In case Alice chooses '0' she will send to Bob a string of k $|0\rangle$'s and $|1\rangle$'s randomly chosen with equal probabilities. In case she chooses '1' she will send to Bob a string of k $|+\rangle$'s and $|-\rangle$'s randomly chosen with equal probabilities. Notice that after the commitment stage Bob has one of the following mixed states:
1) All qubits strings of $|0\rangle, |1\rangle$ of length k, with equal probability.
2) All qubits strings of $|+\rangle, |-\rangle$ of length k, with equal probability.
Since both mixed states have the same density matrix, Bob has no information about Alice's choice.

The reveal stage: Alice classically communicates to Bob her choice and the k bit string she sent in the commitment. Bob measures in the appropriate base ($|0\rangle, |1\rangle$ base in case Alice revealed '0' and $|+\rangle, |-\rangle$ base in case she revealed '1') and compares with the reveal string.

Now, Suppose Alice committed on '0' but revealed '1'. This means that Bob will measure $|0\rangle$'s and $|1\rangle$'s in the $|+\rangle$,$|-\rangle$ base. The probability of getting a $|+\rangle$ or a $|-\rangle$ result when measuring $|0\rangle$'s and $|1\rangle$'s is $\frac{1}{2}$. This implies that Alice has a probability of $\left(\frac{1}{2}\right)^k$ to get away with a reveal, different from the commitment. A probability considered secured.

Apparently, this protocol seems to be secure: Bob has no knowledge about Alice's choice after the commitment stage and Alice has exponentially low probability of getting away with revealing a bit different from the commitment.
Due to the quantum model Alice can perform the protocol without actually committing to anything. Alice can prepare k EPR pairs of the form $|01\rangle - |10\rangle$, and send the first qubit of each pair to Bob. We saw in the first lecture that these states are correlated in every base.
Particularly, $|01\rangle - |10\rangle = |+-\rangle - |-+\rangle$. Now, if Alice wants to convince Bob that she chose '0', she will measure her part of the EPR states in the $|0\rangle, |1\rangle$ base. For a $|0\rangle$ measurement she knows that Bob will measure $|1\rangle$ and for a $|1\rangle$ measurement Bob will measure $|0\rangle$. Thus, she can send a k bits sting that will perfectly comply with Bob's measures. In the same manner Alice can decide to "reveal" '1' by measuring in the $|+\rangle, |-\rangle$ base.

1.2 Bit commitment is impossible

In order to tackle a problem such as showing that a specific protocol is impossible, we need to work with some general definition of the protocol. For a general definition of the bit commitment protocol, we will use the model of two-party quantum protocol given in the following subsection

1.2.1 Two-party quantum protocols

A two party quantum protocol involves two users (Alice and Bob) communicating through a quantum channel C. In such a protocol we consider a direct product H of three Hilbert spaces HA, HB and HC. HA (HB) is the Hilbert space of Alice (Bob) and HC is the Hilbert space of the channel. Initially each of the user's states is pure. During the protocol A and B perform a number of rounds of quantum communication with each other, through the channel. More formally, each of A and B alternately performs a unitary transformation on $HD \otimes HC$, where $D \in \{A, B\}$.

This model is taken from "Why quantum bit commitment and ideal quantum coin tossing are impossible", by Hoi-Kwong and H.F.Chau, in which the authors argue about the generality of the model.

1.2.2 The general definition of the bit commitment protocol

Having understood the two-party quantum protocol we can define the general protocol of bit commitment:
(a) Preparation stage: Alice chooses the value of her commitment to Bob. If b=0 (b=1) she prepares the state $|0\rangle$ ($|1\rangle$) for HA. Bob prepares some state $|BC\rangle$ for the product Hilbert space $HB \otimes HC$. All the states $|0\rangle, |1\rangle$ and $|BC\rangle$ are specified by the protocol and are familiar to both Alice and Bob (Bob, of course, doesn't know which of the states $|0\rangle$ or $|1\rangle$ Alice prepared).
(b) The commitment stage: This step involves a specified and fixed (by the protocol) number of rounds of quantum communication, alternately, between Alice and Bob. According to the two party quantum protocol model each round of quantum communication is actually a unitary transformation on $HD \otimes HC$ ($D \in \{A, B\}$), each such transformation can be generalized to a unitary transformation on the space $H = HA \otimes HB \otimes HC$.
For a secure bit commitment protocol at the end of step (b) Bob has no information about the value of the commitment bit b.
(c) The reveal stage: Once again, Alice and Bob perform a specified and fixed number of rounds of quantum communication, alternately. Each round is modelled as a unitary transformation on $HD \otimes HC$ ($D \in \{A, B\}$), which can be generalized as a unitary transformation on the space $H = HA \otimes HB \otimes HC$.

We note that in a secure protocol the bit Bob learns in step (c) is the actual bit that Alice has committed to in step (b), without any ability to change it.

1.2.3 The impossibility of a secure bit commitment protocol

The impossibility of a secure bit commitment protocol is based on Schmidt decomposition theorem, which in turn is based on the polar and singular decomposition theorems. We give here the proof of Schmidt theorem (All theorems can be found in Michael A. Nielsen and L. Chuang book).

The Singular decomposition theorem: Any matrix C of size $m * n$ can be written as $C = U * D * W$, where U, W are unitary, D satisfies that $D_{ii} \neq 0$ and $D_{ij} = 0$ for $i \neq j$. U is of size $m * m$, D of size $m * n$, and W of size $n * n$.

The Schmidt decomposition theorem:
Let $|\Psi\rangle \in HA \otimes HB$, where H_A is of dimension m, and H_B is of dimension n. $|\Psi\rangle$ can be rewritten as:

$$|\Psi\rangle = \sum_{i=0...\min(m,n)} \sqrt{\lambda_i} * |e_i\rangle \otimes |f_i\rangle$$

where $|e_i\rangle \in HA$, $\langle e_i|e_j\rangle = 0$ for $i \neq j$ and $|f_i\rangle \in HB$, $\langle f_i|f_j\rangle = 0$ for $i \neq j$.

The theorem actually bounds from above by min(m,n), the "amount of correlation" between the Hilbert spaces in the state $|\Psi\rangle$.

Proof:
$|\Psi\rangle \in HA \otimes HB$ and therefore can be written as:

$$|\Psi\rangle = \sum_{i=1...m,\ j=1...n} C_{i,j} |a_i\rangle \otimes |b_j\rangle$$

where $|a_i\rangle, |b_i\rangle$ are orthonormal bases of HA, HB respectively. According to the singular decomposition $C = c_{i,j}$ can be written as
$C = U * D * W$, where U, W are unitary, D satisfies that $D_{i,i} \neq 0$ and $D_{ij} = 0$ for $i \neq j$.
(U is of size $m * m$, D of size $m * n$, and W of size $n * n$).
Since $D_{ij} = 0$ for $i \neq j$, we can write $|\Psi\rangle$ as:

$$|\Psi\rangle = \sum_{k=1...\min(m,n),\ i=1...m,\ j=1...n} U_{i,k} * D_{k,k} * W_{k,j} |a_i\rangle |b_i\rangle$$

Defining $|k_A\rangle \equiv \sum_i U_{i,k}|a_i\rangle$, $|k_B\rangle \equiv \sum_j W_{k,j}|b_j\rangle$ and $\lambda_k \equiv D_{k,k}$, we get:
$|\Psi\rangle = \sum_k \lambda_k |k_A\rangle \otimes |k_B\rangle$, where $|k_A\rangle \in HA$ and $|k_B\rangle \in HB$.

To complete the proof we need to show that $\langle k_A|k'_A\rangle = 0$ and $\langle k_B|k'_B\rangle = 0$ for $k \neq k'$.
$\langle k_A|k'_A\rangle = \langle \sum_i U_{i,k}|a_i\rangle|\sum_i U_{i,k'}|a_i\rangle\rangle = \sum_{i,j} U_{i,k} * \overline{U_{j,k'}}\langle a_i|a_j\rangle$. Since $|a_i\rangle$ is an orthonormal base we get that $\langle k_A|k'_A\rangle = \sum_{i,i} Ui,k * U_{i,k'} = \langle U_k|U'_k\rangle$ - The inner product of the lines k and k' of U. U is unitary and thus this inner product is zero. In the same manner since, $|b_j\rangle$ is an orthonormal base and W is unitary, we get that $\langle k_B|k'_B\rangle = 0$ for $k \neq k'$

Having understood the Schmidt decomposition theorem, we can turn back to proofing the impossibility of the bit commitment protocol.
Let $|\Psi 0\rangle_b$ be the state of $H = HA \otimes HB \otimes HC$ at the end of step (b) in the case Alice chose b=0 And $|\Psi 1\rangle_b$ the state of H in case she chose 1. At the end of stage (b) we can think of the Hilbert space HC as part of the space of the last party who performed a transformation on it. This way we can analyze the state as a two-party state in $HA \otimes HB$. If for example Alice was the last one to perform a transformation on $HA \otimes HC$ then we think of HA as a larger space, which is the tensor product $HA \otimes HC$. The fact that Bob has no information about the value of b implies that the density matrix of his state is independent of the value of b. Formally this means that the reduced density matrix of $|\Psi 0\rangle_b$ to HB equals to the reduced density matrix of $|\Psi 1\rangle_b$ to HB.
Due to the decomposition theorem we can write $|\Psi 0\rangle_b$ and $|\Psi 1\rangle_b$ as follows:

$$|\Psi 0\rangle_b = \sum_k \sqrt{\lambda_k} * |e_k\rangle_A \otimes |f_k\rangle_B$$

$$|\Psi 1\rangle_b = \sum_k \sqrt{\lambda_k} * |e'_k\rangle_A \otimes |f_k\rangle_B$$

where k = min (dim HA, dim HB), $\langle e_k|e_l\rangle = 0$, $\langle e'_k|e'_l\rangle = 0$ and $\langle f_k|f_l\rangle = 0$. Note that the only difference between the states lies in Alice's "elements" of the decomposition: $|e_k\rangle$ and $|e'_k\rangle$, otherwise, Bob has some information about Alice's commitment. More precisely, suppose ρ_0, ρ_1 are the reduced density matrices of $|\Psi 0\rangle_b$, $|\Psi 1\rangle_b$ to HB accordingly.

The fact that the protocol is secure, namely, that Bob has no information about Alice's commitment, means that $\rho_0 = \rho_1$. Now, suppose that

$$|\Psi 0\rangle_b = \sum_k \sqrt{\lambda_k} * |e_k\rangle_A \otimes |f_k\rangle_B$$

$$|\Psi 1\rangle_b = \sum_k \sqrt{\lambda'_k} * |e'_k\rangle_A \otimes |f'_k\rangle_B$$

The probabilities to measure $|e_k\rangle_A$, $|e'_k\rangle_A$ are $|\sqrt{\lambda_k}|^2$, $|\sqrt{\lambda'_k}|^2$, thus we can write

$$\rho_0 = \sum_k \sqrt{\lambda_k} |f_{kA}\rangle\langle f_{kA}|$$

$$\rho_1 = \sum_k \sqrt{\lambda'_k} |f'_{kA}\rangle\langle f'_{kA}|$$

Since $\rho_0 = \rho_1$, both matrices have the same eigenvalues and eigenvectors. For the simple private case where all the λ_k are different, we get that $\lambda_k = \lambda'_k$ and $|f_k\rangle_A = |f'_k\rangle_A$, so that the only difference between $|\Psi 0\rangle_b$, $|\Psi 1\rangle_b$ lies in Alice's "elements".

The fact that the only difference lies in Alice's space means that she can perform a unitary transformation acting on HA alone, and change the whole state of H from $|\Psi 0\rangle_b$ to $|\Psi 1\rangle_b$ and vice versa, thus changing her commitment, without Bob knowing it: Suppose Alice committed to '0' in steps (a), (b). Before step (c) Alice can change the state of H to reflect a commitment to '1' and to go through step (c) revealing '1', thus breaking the security of the protocol, which "demands" that the bit Bob learns in step (c) is the actual bit that Alice has committed to in (b).

1.2.4 freedom in purification

An interesting property rising from the Schmidt decomposition theorem is freedom in purification.
For the definition of purification, suppose ρ_A is a density matrix describing the quantum state of the quantum system A. Purification of ρ_A is a mathematical procedure, in which we introduce another system R and define a pure state $|AR\rangle$ for the system $A \otimes R$, which satisfies that the reduced density matrix of $|AR\rangle$ to A is ρ_A. To show that such a procedure is possible for any state consider the orthonormal decomposition $\rho_A = \sum_i P_i|i_A\rangle\langle i_A|$. To purify ρ_A we introduce a system R, which has the same state space as system A, with orthonormal basis state $|i_R\rangle$. The pure state $|AR\rangle$ for the system $A \otimes R$ is $|AR\rangle = \sum_i \sqrt{P_i}|i_A\rangle \otimes |i_R\rangle$. The reduced density operator for the system A is given by:

$$
\begin{aligned}
Tr_R|AR\rangle\langle AR| &= \sum_{i,j} \sqrt{P_i * P_j} * |i_A\rangle\langle j_A| * Tr(|i_R\rangle\langle j_R|) \\
& \sum_{i,j} \sqrt{P_i * P_j} * |i_A\rangle\langle j_A| * \delta_{i,j} \\
& \sum_{i} P_i * |i_A\rangle\langle i_A| \\
& \rho_A.
\end{aligned}
$$

Suppose $|BA1\rangle$ and $|BA2\rangle$ are two purifications of a state ρ^A to a composite system $A \otimes B$. Freedom in purification means that there exist a unitary operation U_A acting on the system A alone, such that $|BA1\rangle = I_B \otimes U_A|BA2\rangle$.
In our case A is Alice's space and B Bob's space. $|\Psi 0\rangle_b$ and $|\Psi 1\rangle_b$ from the bit commitment protocol are the purifications $|BA1\rangle$ and $|BA2\rangle$. U_A is the unitary matrix that Alice can use to transfer $|e_k\rangle$ to $|e'_k\rangle$ (or vice versa), thus transferring the whole system from $|\Psi 0\rangle_b$ to $|\Psi 1\rangle_b$ (or vice versa).

1.3 Distance measures: Definitions and properties

For the following sections we will need to define distance measures between quantum states.

1.3.1 Fidelity distance

The fidelity distance for the states ρ, σ is defined as:

$$F(\rho, \sigma) \equiv \max |\langle \Psi_0 | \Psi_1 \rangle|$$

where the maximum is taken over all possible purifications Ψ_0, Ψ_1 of ρ, σ.
The fidelity distance holds the following properties:
1) $0 \leq F \leq 1$, $F = 1$ iff $\rho = \sigma$.
2) For any fixed purification Ψ_0 of ρ, there exist a purification Ψ_1 of σ, such that $F(\rho, \sigma) = |\langle \Psi_0 | \Psi_1 \rangle|$

1.3.2 Trace distance

The trace distance for the states ρ, σ is defined as:

$$D(\rho, \sigma) \equiv \frac{1}{2} * tr|\rho - \sigma|.$$

Suppose ρ, σ are diagonal in the same basis, namely, $\rho = \sum_i r_i |i\rangle\langle i|$ and $\sigma = \sum_i s_i |i\rangle\langle i|$. We get that

$$(\rho, \sigma) = \frac{1}{2} * tr| \sum_i (r_i - s_i)|i\rangle\langle i|| = \frac{1}{2} * \sum_i (r_i - s_i)$$

Note that $\frac{1}{2} * \sum_i (r_i - s_i)$ is actually the total variation distance of the probability distributions imposed by the diagonal ρ, σ.
Also Note that $D(\rho, \sigma) \leq 1$, as $\sum_i r_i = 1$ and $\sum_i s_i = 1$.

1.3.3 Non-ideal bit commitment is impossible

By non-ideal bit commitment protocol we suggest that Bob might have a tiny amount of information about Alice's choice after the commitment stage. Noting by $|\Psi 0\rangle_b$, $|\Psi 1\rangle_b$ the overall state of Alice and Bob after the commitment stage in the cases that Alice chose '0', '1' accordingly, and by ρ_0, ρ_1 the reduced density matrices of these states to Bob's space, we formulate the tiny amount of information Bob has, using the fidelity distance, saying that $F(\rho_0, \rho_1) = 1 - \epsilon$. According to property 2 of the fidelity distance for each purification $\Psi 1$ of ρ_1 there is a purification $\Psi 0$ of ρ_0 such that $F(\rho_0, \rho_1) = | \langle \Psi 1 | \Psi 0 \rangle |$. Specifically, for $|\Psi 1\rangle_b$ being a purification of ρ_1 to Alice and Bob mutual space there is a purification Φ_0 of ρ_0 such that $| \langle \Psi 1_b | \Phi_0 \rangle | = F(\rho_0, \rho_1) = 1 - \epsilon$.
Note that both Φ_0 and $|\Psi 0\rangle_b$ are purifications of ρ_0 to Alice and Bob mutual space, where the introduced system used for the purification is Alice's space . Thus due to the freedom of purification there is an unitary transformation Alice can perform AFTER the commitment step and BEFORE the reveal step on her state alone, which turns the overall state from $|\Psi 0\rangle_b$ to Φ_0. This sketches the way in which Alice can cheat:
Alice can starts by committing to '0', so that the overall state will be $|\Psi 0\rangle_b$ by the end of the commitment step. Before the reveal stage she performs an unitary transformation on her state alone to obtain the overall state of Φ_0. Since $| \langle \Psi 1_b | \Phi_0 \rangle | = 1 - \epsilon$ The reduced density matrix of Φ_0 is very close to ρ_1, so Bob can hardly detect that Alice cheated. Alice can proceed now with the reveal stage, revealing '1'.

1.4 Quantum coin tossing

Quantum coin tossing is a two party protocol satisfying the following:
1) The outcome of the protocol is '0', '1' or 'invalid'.
2) Both parties know the outcome.
3) If the outcome is '0' or '1', both parties can be sure that they occurred with precise probabilities P,1-P given by the protocol.
4) If both users are honest, the outcome 'invalid' will never occur.

It is an open question, whether there is a coin flipping protocol, which gives ϵ certainty in property 3. It is known that such a protocol demands unbounded number of communication rounds.

Following is a $(\frac{3}{4}, \frac{1}{4})$ biased coin tossing protocol, namely, the probabilities P, 1-P mentioned in property 3 of the protocol are $\frac{3}{4}$, $\frac{1}{4}$.
Alice and Bob work in the base $|0\rangle, |1\rangle, |2\rangle$.

(a) Alice randomly chooses bits b and x.
(b) In the case that b=0 Alice will send Bob $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ for x=0 and $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ for x=1. In case b=1 she will send Bob $\frac{|0\rangle+|2\rangle}{\sqrt{2}}$ for x=0 and $\frac{|0\rangle-|2\rangle}{\sqrt{2}}$ for x=1.
(c) Bob chooses randomly the bit b' and sends it to Alice.
(d) Alice sends Bob b,x from step (b).
(e) Bob measures the state he received from Alice. In case the measurement comply with b,x the protocol ends successfully with $b \oplus b'$, otherwise Bob aborts.

2 Quantum Key distribution

In key distribution protocol the "users" start with no pre-shared knowledge and end with a secret key, while all communication was via an insecure channel. To understand the quantum Key distribution we need two tools: random sampling and the entanglement purification protocol described below.

2.1 Random sampling

Let $S = 0^{2n}$. Suppose that S is transferred via a noisy channel and received as S'. S' is sampled in n random positions. The probability of sampling less then $\delta * n$ $1's$ on the sampled bits and having more then $(\delta + \epsilon) * n$ $1's$ on the rest of the bits is less then $e^{-O(\epsilon^2 n)}$.
For the quantum analogue, suppose that Alice prepared the state $|\Phi^+\rangle^{\bigotimes 2n}$ and sent the second halves of each pair to Bob. Now they both measure n random qubits to find out that there are less then $\delta * n$ errors. This implies that the fidelity of the rest n qubits and the state defined by $\delta * n$ errors on the original n qubits, is exponentially close to 1.
In our case the noise is due to eavesdropping done on the qubits Alice sends to Bob.

2.2 Entanglement Purification Protocol

The key idea of the entanglement purification protocol is that measuring the error syndromes according to one CSS code results in a code word of another CSS code. To explain the entanglement purification protocol we need the following definitions and notations:
1) Denote Q as a $CSS(C1, C2)$ code, where $C1$ and $C2^{\perp}$ are classic error correcting codes, correcting up to t errors. Also Q encodes m qubits using n qubits.
2) Denote $H1$ as the parity check matrix for the code $C1$ and $H2$ the parity check matrix for $C2^{\perp}$.

Recall that the quantum code $CSS(C1, C2)$ is defined as the vector space spanned by the states $|v + C2\rangle$, where $v \in C1$, namely, a state $v \in C1$ is encoded by:

$$\frac{1}{\sqrt{|C2|}} * \sum_{w \in C2} |v + w\rangle$$

3) We define the code $Q_{x,z}$ parameterized by n bits binary vectors x, z as follows: The state $v \in C1$ is encoded by

$$\frac{1}{\sqrt{|C2|}} * \sum_{w \in C2} (-1)^{z*w} |v + w + x\rangle$$

Note that the code words in $Q_{x,z}$ are the results of applying bit flips and phase flips according to the binary vectors x, z on words in Q. bit flips (phase flips) are applied where there are $1's$ in x (z).
Also note that the code $Q_{x,z}$ has the same error correcting properties as Q (it encodes the same number of qubits, and can correct the same number of errors).
For each x, z, $Q_{x,z}(v)$ is a superposition of strings c. According to the definition of $Q_{x,z}(v)$ each such string c in the superposition has the same syndrome according to Q.
In other words if we take the state $\sum_{x,z} \sum_v |Q_{x,z}(v)\rangle$, where $v \in C1$, and we measure the bit flip and the phase flip syndromes according to Q, we end up with a superposition of all strings with the measured bit and phase flip syndromes, i.e.

$$\sum_{x',z'} \sum_v |Q_{x,z}(v)\rangle$$

for all x', z' with the same syndrome.
Now, if we started with state

$$\sum_{x,z} \sum_v |Q_{x,z}(v)\rangle$$

with $x \in Z_2^n/C1,\ z \in Z_2^n/C2^{\perp}$ (instead of all x, z), measuring the syndrome according to Q will result in

$$\sum_v |Q_{x,z}(v)\rangle$$

for some specific x, z.

As shown later, $|\Phi^+\rangle^{\bigotimes 2n} = \sum_{x,z} \sum_v |Q_{x,z}(v)\rangle |Q_{x,z}(v)\rangle$,
where $x \in Z_2^n/C1, z \in Z_2^n/C2^{\perp}, v \in C1$.
Suppose Alice and Bob share the state $|\Phi^+\rangle^{\bigotimes 2n}$ of pure n EPR pairs. Measuring the error syndromes according to Q will result in the state

$$\sum_v |Q_{x,z}(v)\rangle |Q_{x,z}(v)\rangle$$

Which is the encoding of $|\Phi^+\rangle^{\bigotimes m}$ according to $Q_{x,z}$

Now, if Alice and Bob share the state $\epsilon|\Phi^+\rangle^{\bigotimes m}$, where ϵ is an application of no more then t bit flips and no more then t phase flips on Bob's qubits then by comparing their syndrome measurements they can detect the exact location of the errors and correct it to obtain $|\Phi^+\rangle^{\bigotimes m}$ encoded by $Q_{x,z}$ code, where x, z are known.
To complete the protocol we prove the equation:

$$|\Phi^+\rangle^{\bigotimes 2n} = \sum_{x,z}\sum_{v}|Q_{x,z}(v)\rangle|Q_{x,z}(v)\rangle$$

where $x \in Z_2^n/C1, z \in Z_2^n/C2\bot, v \in C1$.
Ommiting the fuctors we have:

$$\begin{aligned}\sum_{x,z}\sum_{v}|Q_{x,z}(v)\rangle|Q_{x,z}(v)\rangle &= \sum_{x,z,v}\sum_{w\in C2}(-1)^{z\cdot w}|x+w+v\rangle)(\sum_{w\in C2}(-1)^{z\cdot w}|x+w+v\rangle)) \\ & \sum_{x,z,v,w,w'}(-1)^{z\cdot(w+w')}|x+w+v\rangle|x+w'+v\rangle\end{aligned}$$

Summing over all z we get something of the form:

$$\sum_{z}(-1)^{z\cdot(w+w')}|\Psi\rangle|\Psi\rangle$$

Note that this sum is zero for $w \neq w'$. Thus we get:

$$\sum_{x,v,w}|x+w+v\rangle|x+w+v\rangle = \sum_{v}|v\rangle|v\rangle = |\Phi^+\rangle^{\bigotimes 2n}$$

2.3 The key disribution protocol

Suppose Alice and Bob share m bits in the $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ EPR state. By measuring these qubits they get a random m bits key uniformly distributed. The only problem with the naive approach of Alice preparing m qubits in the EPR state and sending half of them to Bob is Eve doing eavesdropping in the middle. The idea behind the following protocol is using the random sampling bound, to estimate Eve's amount of eavesdropping. In case the eavesdropping amount is not too big Alice and Bob can use the entanglement purification protocol to "translate" Eve's errors (caused by the eavesdropping) to a perfect m EPR pairs encoded in a certain CSS code.

Following is the protocol:
Denote $|\Phi^{\pm}\rangle = |00\rangle \pm |11\rangle$ and $|\Psi^{\pm}\rangle = |01\rangle \pm |10\rangle$. Suppose Alice and Bob share a CSS code for fixing t bit and phase flips. Denote $\delta = \frac{n}{t}$.

(a) Alice prepares the state $|\Phi^{+}\rangle^{\bigotimes 2n}$, and sends Bob 2n halves of these EPR pairs
(b) Bob receives the qubits and publicly announces this fact.
(c) Alice chooses n positions at random and sends them to Bob. (We denote the qubits at these positions as "check bits").
(d) Alice announces for each "check bit", whether it should be measured in the standard basis or in the Hadamard basis.
(e) Alice and Bob measure the n "check bits" accordingly.
(f) Alice publishes her measurement results.
(g) In case less then $\delta * n$ phase flips and less then $\delta * n$ bit flips happened, Bob announces "continue", otherwise he announces "abort".
(h) Alice and Bob perform the entanglement purification protocol for getting m perfect $|\Phi^{+}\rangle$ EPR pairs (taking $t = \delta * n$).
(i) Alice and Bob measure their m perfect $|\Phi^{+}\rangle$ EPR pairs to share a random m bit key.

The security of the protocol is based on the following argument. Any eavesdropping can acts on each of the original state's qubit as follows:
X $|\Phi^+\rangle = |\Psi^+\rangle$ (bit flip on Bob's half).
Z $|\Phi^+\rangle = |\Phi^-\rangle$ (phase flip on Bob's half).
XZ $|\Phi^+\rangle = |\Psi^-\rangle$ (bit and phase flips on Bob's half).

In steps (c) - (g) Alice and Bob sample the amount of eavesdropping, which could have occurred in step (a). This is done by measuring the n randomly "check bits" in either the standard basis or the Hadamard basis. Since $|\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-| = |01\rangle\langle 01| + |10\rangle\langle 10|$ and
$|\Phi^-\rangle\langle\Phi^-| + |\Psi^-\rangle\langle\Psi^-| = |+-\rangle\langle +-| + |-+\rangle\langle -+|$,
Alice and Bob can find out from their measurements in the standard and Hadamard basis whether a bit flip or a phase flip was "applied", and thus knowing in step (g) that no more then $\delta * n$ bit flips and no more then $\delta * n$ phase flips happened. Also in steps (f) - (g) Alice and Bob know, where exactly the errors have occurred. Knowing which errors occurred and where is important for the entanglement purification protocol.

By the random sampling bound the fact that Bob declared "continue" in step (g), it is promised that the entanglement purification protocol will work with very high probability.