Quantum Key Distribution Lab 1

Raul-Martin Rebane

April 21, 2020

1 Bell pairs

To describe Bell pairs we use the following notation:

$$
\begin{aligned}
|\beta_{00}\rangle &= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \\
|\beta_{01}\rangle &= \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle \\
|\beta_{10}\rangle &= \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle \\
|\beta_{11}\rangle &= \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle
\end{aligned}
$$

At the start of the protocol, Alice generates a lot of $|\beta_{00}\rangle$ qubits and sends the right half of each pair to Bob. Because she sends one qubit from each pair, this becomes notationally tricky, as there is some shuffling of qubits around. Because of this we introduce the notation

$$|\tilde{xy}\rangle = |\beta_{x_1 y_1}\rangle \otimes |\beta_{x_2 y_2}\rangle \otimes \ldots \otimes |\beta_{x_n y_n}\rangle$$

So x contains the first bit of every β and y contains all of the second bits. The most important state for us is the one that Alice prepares in the start.

$$|\widetilde{0\_0}\rangle = |\beta_{00}\rangle \otimes |\beta_{00}\rangle \otimes \ldots \otimes |\beta_{00}\rangle$$

Note that this state is an equal superposition of all n-bit computational states, duplicated for Alice and Bob. This might not be obvious first, so let's look at a specific case of $n = 2$.

$$
\begin{aligned}
|\widetilde{0\_0}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
&= \frac{1}{2}|0000\rangle + \frac{1}{2}|0011\rangle + \frac{1}{2}|1100\rangle + \frac{1}{2}|1111\rangle
\end{aligned}
$$

These states look a little odd, but that's because in reality Alice sends one qubit from each *pair* to Bob, so the qubits of Alice and Bob are interlaced in that sum. So if we were to annotate $|0011\rangle$ to show who has what qubit, it's actually $|0_A 0_B 1_A 1_B\rangle$. So if shuffle the qubits around so that the first n qubits belong to Alice and the rest to Bob, $|0011\rangle$ becomes $|01\rangle \otimes |01\rangle$. Thus, with the qubits rearranged, the sum we have above is:

$$\frac{1}{2}|00\rangle \otimes |00\rangle + \frac{1}{2}|01\rangle \otimes |01\rangle + \frac{1}{2}|10\rangle \otimes |10\rangle + \frac{1}{2}|11\rangle \otimes |11\rangle +$$

And in the general case we can write:

$$|\widetilde{0\_0}\rangle = \sum_{k\in\{0,1\}^n} \frac{1}{2^{n/2}}|k\rangle \otimes |k\rangle$$

There are some important things to note about Bell pairs. For one, they form an orthonormal basis. This means that whatever state Alice and Bob end up in, it is possible to express it in some linear combination of Bell pairs.

The other important thing to note, is that it is possible to go from any non-$|\beta_{00}\rangle$ state into $|\beta_{00}\rangle$ by only having one party do all of the work. $|\beta_{01}\rangle$ can be turned to $|\beta_{00}\rangle$ by performing the X-gate on the second qubit. For $|\beta_{10}\rangle$ we need to apply the Z-gate on the second qubit. And for $|\beta_{10}\rangle$ we perform both on the second qubit. But since we always only do operations on the second qubit, then no matter what Bell state we start with, we only apply a unitary on the second qubit.

$$|\beta_{ij}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes X^j Z^i|0\rangle + |1\rangle \otimes X^j Z^i|1\rangle) = I \otimes (X^j Z^i)|\beta_{00}\rangle$$

And if we have many of these pairs, then in the reordering we can express $|\widetilde{xy}\rangle$ as a $|\widetilde{0\_0}\rangle$ that has had a unitary applied to the second half of the qubits.

$$|\widetilde{xy}\rangle = \sum_{k\in\{0,1\}^n} \frac{1}{2^{n/2}}|k\rangle \otimes U|k\rangle$$

2 Testing the Bell pairs

Because Alice sends Bob the half of each Bell pair over an insecure channel, Eve might introduce some errors by interacting with the system. To detect this, Alice and Bob randomly sample some of their qubits to see if they have been tampered with. This process is described in Lecture 9, but for the purposes of this lab, what's important is that after sampling and throwing away some qubits, we are left with fewer qubits, but we know that these have at most t errors. By errors we mean the number of indices where the Bell pair is no longer $|\beta_{00}\rangle$.

$$|xy| := |\{i : x_i y_i \neq 00\}|$$

And so if we are guaranteed to have at most t errors, we know that our state is:

$$\sum_{|xy| \leq t} \lambda_{xy} |\widetilde{xy}\rangle \otimes |\Psi_{E_{xy}}\rangle$$

The reason we can write the state as a superposition like this is because the Bell states form an orthonormal basis, and so if there is an error with pair i (it is no longer $|\beta_{00}\rangle$), then it can still be expressed as a linear combination of all $|\beta_{ij}\rangle$.

3 Lab exercise: Guessing the key

3.1 When no errors are introduced

For our first exercise, let's see what is the probability that Eve can guess the key of Alice. To start with, let's assume that Eve introduces no errors, and her system is entirely independent from Alice and Bob's system.

In that case, our composite system has state

$$|\Psi\rangle = |\widetilde{0\_0}\rangle \otimes |\Psi_E\rangle$$

What we're interested in is if Alice's and Eve's registers are both measured, are their keys the same? We want to quantify $\Pr[K_A = K_E]$. However, how are we going to design a projector that measures that Alice and Eve's registers are the same? We know that Alice is going to measure her register in the computational basis, so we can do the same for Eve's register. And what we want is that Alice's result k is also on Eve's register. And the sum of all possible k's gives us the total probability that the keys are equal.

$$\Pr[K_A = K_E] = \sum_{k \in \{0,1\}^n} \Pr[K_A = k \wedge K_E = k] = \sum_{k \in \{0,1\}^n} ||P_k |\Psi\rangle||^2$$
$$P_k := |k\rangle\langle k| \otimes I \otimes |k\rangle\langle k|$$

Where P_k is the projector which measures whether Alice and Eve's registers are both k. The $||P_k|\Psi\rangle||^2$ is just a projective measurement on a quantum state (not a density operator).

From the previous section we know that $|\widetilde{0\_0}\rangle$ is an equal superposition of computational basis states, and so we can express $|\Psi\rangle$ as

$$|\Psi\rangle = |\widetilde{0\_0}\rangle \otimes |\Psi_E\rangle = \sum_{z\in\{0,1\}^n} \frac{1}{2^{n/2}}|z\rangle \otimes |z\rangle \otimes |\Psi_E\rangle$$

Now we have our state in a three-part state, to which we can apply P_k

$$\sum_{k\in\{0,1\}^n} ||P_k \sum_{z\in\{0,1\}^n} \frac{1}{2^{n/2}}|z\rangle \otimes |z\rangle \otimes |\Psi_E\rangle||^2 =$$
$$= \sum_{k\in\{0,1\}^n} || \sum_{z\in\{0,1\}^n} \frac{1}{2^{n/2}}|k\rangle\langle k||z\rangle \otimes I|z\rangle \otimes |k\rangle\langle k||\Psi_E\rangle||^2$$

Once again we have something in the form of $\langle k||z\rangle$. Since k and z are basis states, they're either equal (in which case the inner product is 1) or orthogonal (which means their inner product is 0). Note that this would **not** hold for a general $\langle z||\Psi\rangle$ where $|\Psi\rangle$ could be any superposition of basis states.

But since in our case they are basis states, only the $z = k$ terms remain, which means we can get rid of the inner sum.

$$\sum_{k\in\{0,1\}^n} || \sum_{z\in\{0,1\}^n} \frac{1}{2^{n/2}}|k\rangle\langle k||z\rangle \otimes I|z\rangle \otimes |k\rangle\langle k||\Psi_E\rangle||^2 =$$
$$= \sum_{k\in\{0,1\}^n} ||\frac{1}{2^{n/2}}|k\rangle \otimes |k\rangle \otimes |k\rangle\langle k||\Psi_E\rangle||^2$$

Now, since $|\Psi_E\rangle$ can be any state, we can't apply the same technique as before. But since we know all of the k's form an orthonormal basis, $|\Psi_E\rangle$ is expressible in that basis $|\Psi_E\rangle = \lambda_{0\ldots0}|0\ldots0\rangle + \ldots + \lambda_{1\ldots1}|1\ldots1\rangle$ and it has norm $\sum_k ||\lambda_k||^2 = 1$. But this is exactly what we have in the above sum as $\langle k||\Psi_E\rangle = \lambda_k$. Moving the $\frac{1}{2^{n/2}}$ then gives us our final answer.

$$\sum_{k\in\{0,1\}^n} ||\frac{1}{2^{n/2}}|k\rangle \otimes |k\rangle \otimes |k\rangle\langle k||\Psi_E\rangle||^2 =$$
$$= \frac{1}{2^n} \sum_{k\in\{0,1\}^n} |||k\rangle \otimes |k\rangle \otimes |k\rangle\langle k||\Psi_E\rangle||^2 = \frac{1}{2^n} \cdot 1$$

3.2 With errors

Now let's look at the case where Eve does interact with the system and can introduce some errors into Alice and Bob's pairs. From the Bell pair testing part, we know that after testing some Bell pairs, we have a system with at most t errors. We also know that the Bell pairs form an orthonormal basis, and so we can write our state as

$$|\Psi\rangle = \sum_{|xy|\leq t} \lambda_{xy} |\widetilde{xy}\rangle \otimes |\Psi_{E_{xy}}\rangle$$

Note that we have $|\Psi_{E_{xy}}\rangle$ because Eve's state is allowed to depend on the errors she introduces. Using the same reasoning as before, we can sum over the possible results k.

$$\sum_{k\in\{0,1\}^n} \Pr[K_A = k \wedge K_E = k] = \sum_{k\in\{0,1\}^n} || \sum_{|xy|\leq t} \lambda_{xy} P_k |\widetilde{xy}\rangle \otimes |\Psi_{E_{xy}}\rangle||^2$$

Here to get the lambda coefficients out, we will just use a known inequality. This is not something you need to know in the exam, it's just needed in this computation.

$$\sum_i ||a_i \Psi_i||^2 \leq (\sum_i |a_i|^2)(\sum_i ||\Psi_i||^2)$$

Applying this inequality allows us to remove the lambdas. We can remove them after applying the inequality because they are the coefficients of a superposition and thus by definition $\sum_{|xy|\leq t} |\lambda_{xy}|^2 = 1$. We now apply the inequality, remove the lambdas, and rearrange the sum.

$$\begin{aligned}\sum_{k\in\{0,1\}^n} || \sum_{|xy|\leq t} \lambda_{xy} P_k |\widetilde{xy}\rangle \otimes |\Psi_{E_{xy}}\rangle||^2 \leq &\sum_{k\in\{0,1\}^n} (\sum_{|xy|\leq t} |\lambda_{xy}|^2)(\sum_{|xy|\leq t} ||P_k|\widetilde{xy}\rangle \otimes |\Psi_{xy}\rangle||^2) = \\ = &\sum_{k\in\{0,1\}^n} \sum_{|xy|\leq t} ||P_k|\widetilde{xy}\rangle \otimes |\Psi_{xy}\rangle||^2 = \\ = &\sum_{|xy|\leq t} \sum_{k\in\{0,1\}^n} ||P_k|\widetilde{xy}\rangle \otimes |\Psi_{xy}\rangle||^2\end{aligned}$$

Rearranging the sum makes the inner sum look a lot like what we had before. The only difference is that instead of $|\widetilde{0\_0}\rangle$ we have $|\widetilde{xy}\rangle$. However, remember that we can turn any $|\widetilde{xy}\rangle$ into $|\widetilde{0\_0}\rangle$ by only applying a unitary to one qubit of the pair. In our case, let's have Bob do all of the unitary transformations.

$$\sum_{|xy|\leq t} \sum_{k\in\{0,1\}^n} ||P_k|\widetilde{xy}\rangle \otimes |\Psi_{xy}\rangle||^2 = \sum_{|xy|\leq t} \sum_{k\in\{0,1\}^n} ||P_k \frac{1}{2^{n/2}} \sum_{z\in\{0,1\}^n} |z\rangle \otimes U|z\rangle \otimes |\Psi_{xy}\rangle||^2$$

Now this allows us to apply the projector directly, and proceed exactly as we did in the simpler case, removing the z sum using $\langle k||z\rangle$ and then using $\sum_k ||\langle k||\Psi_{E_{xy}}\rangle||^2 = 1$.

$$\sum_{|xy|\leq t}\sum_{k\in\{0,1\}^n} ||\frac{1}{2^{n/2}}\sum_{z\in\{0,1\}^n} |k\rangle\langle k||z\rangle \otimes IU|z\rangle \otimes |k\rangle\langle k||\Psi_{xy}\rangle||^2 =$$

$$= \frac{1}{2^n}\sum_{|xy|\leq t}\sum_{k\in\{0,1\}^n} |||k\rangle \otimes U|k\rangle \otimes |k\rangle\langle k||\Psi_{xy}\rangle||^2 = \frac{1}{2^n}\sum_{|xy|\leq t} 1 = \frac{|M|}{2^n}$$

Since we have a 1 for every bitstring with up to t errors, our final result is $\frac{|M|}{2^n}$ where M is the set of all bitstrings with up to t errors.