A Solution to R&P 2.10

In this problem we're asked to consider the BB84 protocol in the case that Eve doesn't know which two bases to choose from, and so she chooses a basis at random. The important input is the angle between her basis and Alice's, so without loss of generality we can consider the case in which Alice encodes a bit with the standard basis,

$$0 \to |0\rangle, \quad 1 \to |1\rangle.$$

Eve will use the basis

$$|v\rangle = \cos\theta|0\rangle - \sin\theta|1\rangle, \quad |v_\perp\rangle = \sin\theta|0\rangle + \cos\theta|1\rangle,$$

assigning the bit value 0 to $|v\rangle$ and 1 to $|v_\perp\rangle$. We could in principle include a relative phase factor $e^{i\phi}$ between the $|0\rangle$ and $|1\rangle$ of $|v\rangle$, but let's not for now. We'll consider the range $0 \leq \theta \leq \pi/2$.

(a) *On average, what percentage of bit values of the final key will Eve know for sure after listening to Alice and Bob's conversation on the public channel?*

Zero. I'm open to other lines of thinking on this one, but as far as I understand, Eve can only be certain of bit values when she has used the same basis as Alice for her measurement. There is only one angle θ (namely $\theta = 0$) at which her random basis could align with Alice's, out of a continuum of possible angles. The probability of hitting a point on a continuum is zero. If Eve wanted to accept a non-zero percentage of bits, she could set a bound on her uncertainty and determine how close her alignment would need to be to Alice's to meet that bound.

(b) *On average, what percentage of bits in her string are correct?*

If Alice sends a 0, the probability that Eve measures a 0 is (remembering that for Eve, $0 \leftrightarrow |v\rangle$)

$$P(0) = |\langle v|0\rangle|^2 = \cos^2\theta.$$

Likewise, if Alice sends a 1, the probability that Eve measures a 1 is

$$P(1) = |\langle v_\perp|1\rangle|^2 = \cos^2\theta.$$

The average of $\cos^2\theta$ over the possible angles is

$$\frac{1}{\pi/2}\int_0^{\pi/2} \cos^2\theta \, d\theta = 1/2.$$

Eve does worse (an average success rate of 1/2 vs. 3/4 from the old scenario) when she doesn't know the bases Alice is using.

(c) *How many bits do Alice and Bob need to compare to have a 90 percent chance of detecting Eve's presence?*

To detect possible eavesdropping, Alice and Bob compare bits they should be able to trust, i.e. those where they used the same basis. So we consider a bit where Bob used the same basis as Alice, which again without loss of generality we take to be the standard basis. The question is, what is the chance that Bob receives a correct bit value even though Eve was tampering? Suppose Alice sends a 0. There are two ways Bob could receive a 0:

1. Alice sends a 0, Eve receives a 0 (in her basis), Bob receives a 0.
2. Alice sends a 0, Eve receives a 1 (in her basis), Bob receives a 0.

In expressions that follow we read from right to left – Alice sends a bit (ket), Eve receives it in her basis (bra), then Eve resends it using her basis (ket), and finally Bob receives it (bra). The probabilities for the two possibilities are

1. $|\langle 0|v\rangle\langle v|0\rangle|^2 = \cos^4\theta$.
2. $|\langle 0|v_\perp\rangle\langle v_\perp|0\rangle|^2 = \sin^4\theta$.

If Alice had sent a 1 instead, we would similarly have found that Bob would receive the correct value with probability $\cos^4\theta + \sin^4\theta$.

The probability that Bob receives n bits in row correctly, despite Eve's tampering, is

$$(\cos^4\theta_1 + \sin^4\theta_1) \cdot (\cos^4\theta_2 + \sin^4\theta_2) \cdot \ldots \cdot (\cos^4\theta_n + \sin^4\theta_n).$$

It's the product of the probabilities for each of the n bits, remembering that θ varies randomly from one bit to the next. If Bob is to be 90% confident there was no tampering, this product, which represents the probability of undetected tampering, has to be less than 0.1 (or 10%). But what to put for the θ_i?

Here my understanding of probability theory gets sketchy, but I think there's a rule that if the probability for a given θ goes as $\cos^4\theta + \sin^4\theta$, then the overall probability that Bob gets a correct bit is given by averaging that function over θ.

The average value of $\cos^4\theta + \sin^4\theta$ on the interval is

$$\frac{1}{\pi/2}\int_0^{\pi/2} \cos^4\theta + \sin^4\theta \, d\theta = 3/4.$$

So as in the old scenario where Eve knew the bases Alice and Bob were using, we compute[1]

$$\left(\frac{3}{4}\right)^n < 0.1 \Longrightarrow n > \frac{\log(0.1)}{\log\left(\frac{3}{4}\right)} \approx 8.$$

[1]Remember that we flip a less-than sign to a greater-than sign when we divide by a negative number. Here, $\log\left(\frac{3}{4}\right) \approx -.29$.