ch 8 quantum crypto exercise sheet

Alice, Bob, Eve use this quantum cryptography scheme from Singh: Filter 0 is rectilinear `+` , filter 1 is diagonal `x` . For `|,-` spins, 0 is `-` and 1 is `|`; for `\,/` spins, 0 is `\` and 1 is `/`. We assume photons have the four spins, or polarisations, or states, mentioned, which we name as follows: `|` "vertical" `-` "horizontal" `/` "upright diagonal" `\` "upleft diagonal". The table below summarizes our binary naming of filters and spins.

	0	1
filter	`+`	`x`
spin	`-`	`|`
spin	`\`	`/`

If the correct filter (`+` for `- |`, `x` for `\ /`) is used, then the photon is measured correctly. If the incorrect filter is used, then the photon is altered with prob .5 each to one of the two spins of that filter. E.g. if the `x` is used with photon with spin `|`, then, with prob .5, the photon is measured as (and deflected into) a photon with spin `\`; with prob .5, the photon is measured as (and deflected into) a photon with with spin `/`.

1. Alice generates two (pseudo)random n bit strings from a uniform equiprobable 0/1 distribution: 1101 1100 1110 1101 0100 0000 and 0010 0000 1110 0010 0001 0110. She uses the first string for filter selection and the second string for key construction.

   What photon sequence does she send to Bob?

2. What does Bob do next? If Bob needs a random string, use

   1000 0001 0100 0111 0101 0010.

3. What happens next? What key is created by Alice and Bob?

4. Assume Eve eavesdropped, using string 1101 1110 1011 0011 0010 1010 for filter selection. Show the parts of Alice's message that Even can read.

5. Alice and Bob decide to sacrifice the 1st four bits of their created key in order to check for eavesdropping. What happens next? What is the result if Eve did not eavedrop? What is the result if Eve did eavesdrop, using the filter string mentioned above?

1.
```
string    1101 1100 1110 1101 0100 0000
filter    xx+x xx++ xxx+ xx+x +x++ ++++
message   0010 0000 1110 0010 0001 0110
photon    \\|\ \\-- ///- \\|\ -\-| -||-
```

2. Bob uses the random string to pick a filter sequence which he uses to measure the photon sequence:

```
string    1000 0001 0100 0111 0101 0010
filter    x+++ +++x +x++ +xxx +x+x ++x+
photon    \\|\ \\-- ///- \\|\ -\-| -||-
result    \?|? ??-? ?/?- ?\?\ -\-? -|?-
msg       0?1? ??0? ?1?0 ?0?0 000? 01?0
```

3. Alice and Bob share their filter sequences over an insecure channel. They find that they used the same filters in positions 1 3 7 10 12 14 16 17 18 19 21 22 24. So together they have generated this key: 0 1 0 1 0 0 0 0 0 0 0 1 0

4.
```
string    1101 1110 1011 0011 0010 1010
filter    xx+x xxx+ x+xx ++xx ++x+ x+x+
photon    \\|\ \\-- ///- \\|\ -\-| -||-
result    \\|\ \\?- /?/? ???\ -??| ?|?-
msg       0010 00?0 1?1? ???0 0??1 ?1?0
```

   So Eve has the correct answer in positions 1 2 3 4 5 6 8 9 11 16 17 20 22 24. So she knows these parts of the joint Alice-Bob key:

```
1  3  7 10 12 14 16 17 18 19 21 22 24
0  1  0  1  0  0  0  0  0  0  0  1  0
0  1  ?  ?  ?  ?  0  0  ?  ?  ?  1  0
```

5. Alice and Bob sacrifice the first 4 bits. So Alice tells Bob that for positions 1,3,7,10 she used photons `\ | / -`. Bob says that those are the photons that he measured.

   If Eve has eavesdropped as above, then Eve used the wrong filters in positions 7 and 10. In each case she would have altered the photon. Then Bob's measuring would also have altered the photon. There is a .5 chance in each case that the resulting two alterations would lead back to the correct original spin, and a .5 chance that they would lead to the wrong spin. So there is a .5 chance in each case that Bob notices Eve's eavesdropping. So, with probability `.5*.5=.25` Bob does not detect Eve's intervention, with probability `1-.25=.75` Bob does notice. If Bob does notice, then Alice and Bob throw away the key.

   Of course, if Bob and Alice want more security, they would sacrifice more bits.

   In general, if they agree to sacrifice k bits, then (on average) Eve will guess the wrong filter in .5 of these cases, so the probability that Eve is detected is $1 - 2^{k/2}$.