THE OPEN UNIVERSITY

SXP390 Tutor Marked Assignment 03 - Part 4

William Ockmore

August 27, 2016

1 The BB84 and B92 prepare and measure protocols

1.1 BB84

The BB84 protocol was the first proposed QKD protocol, put forward as the name implies in 1984 by Bennet and Brassard in their paper.

1.1.1 The protocol

In BB84, Alice uses a single photon source to transmit a set of states to Bob, encoded in the polarization of the photons. Both Alice and Bob agree to align their polarizers in either the vertical/horizontal (×) basis, or the complementary basis of +45/-45 (+). Alice then transmits a set of photons down the quantum channel, randomly choosing one of the two bases for each photon, whilst Bob measures in his choice of basis for each photon received.

$$\begin{array}{rcl} |H\rangle & \text{codes for} & 0_+ \\ |V\rangle & \text{codes for} & 1_+ \\ |{+45}\rangle & \text{codes for} & 0_\times \\ |{-45}\rangle & \text{codes for} & 1_\times \end{array}$$

Both Alice and Bob now have a list of sent of received bits, each with a basis. The second phase of the protocol is the classical sifting step: over the unsecured classical channel, they first start by comparing which bases were used for each bit, and discarding the bits for which they used different bases. For a list of size N this step will on average reduce its size by half, to $N/2$. Having matched the measurement basis, this list is referred to as the *raw key.*

Alice and Bob now reveal a random sample of their raw key to one another, to compare for errors. By comparing each bit publicly over the classical channel, they can estimate the error rate for the quantum channel. If no errors are found, the raw key is already the secret key. If there are errors, Alice and Bob must either correct for them or discard their key INSERT REFERENCE. Both these actions can take place over the classical channel; hence this step is called the *classical post-processing.* At the end of this phase, depending on how much information Eve could possess, Alice and Bob either share a secret key or they must discard the potentially compromised key.

1.2 B92

The B92 protocol, involving just 2 non-orthogonal states, is the most minimalist QKD protocol in terms of encoding. Described by Bennet in 1992, the B92 coding allows the receiver to learn whenever they get the bit sent without further discussion from Alice. Although sometimes easier to implement than the more popular BB84, it is more difficult to establish unconditional security in the case of B92, as it is much more sensitive to noise in the quantum channel.

1.2.1 The protocol

B92 can be carried out using the two bases used in BB84. Following on from the above description, Alice sends either $|H\rangle$ or $|{+45}\rangle$, and Bob chooses to measure the incoming bit in either the $(\times)$ or the $(+)$ basis. Both of these states code for 0 in BB84; if Bob measures the state that codes for 1 ($|{-45}\rangle$ or $|V\rangle$ respectively) he can be certain that Alice transmitted her bit in the opposite basis. Hence, B92 allows the participants to restrict their transmissions in the sifting phase to whether or not Bob made a conclusive measurement for each bit sent. After discarding all bits for which Bob cannot be certain, the raw key they are left with is on average $N/4$ bits long, for an initial transmission of N bits.

After a simple comparison of raw key length to the length of the initial string sent by Alice for the classical post processing step, the participants either possess a secret key, or have been alerted to the possibility of Eve's presence.

2 Limitations of QKD - Eavesdropping techniques

In most literature on QKD, Eve is assumed for the completeness of security proofs to have no restrictions on her eavesdropping, other than the fundamental limitations of quantum mechanics itself; namely, the no-cloning theorem and the effects of measurement on a free particle. Briefly described here are the most commonly considered eavesdropping techniques that are considered for BB84 and B92.

2.0.1 Intecept-resend

Potentially the most straightforward eavesdropping technique generally considered is the intercept-resend strategy, which functions exactly the same for both BB84 and B92. Eve essentially takes the same actions as Bob; with her unrestricted capabilities, performs a quantum non-demolition measurement on the incoming photons from Alice, measuring in either the $\times$ or the $+$ basis. If she has measured in the basis used by Alice, the photon continues on to Bob, and Eve has obtained full information whilst introducing no errors to the signal. However, if she has measured in the wrong basis, her result will be uncorrelated with Alice's; meanwhile, she will have sent along a modified state, so even if Bob measures in the same basis as sent by Alice, half the time he will get the wrong result.

Intercept-resend leaves Eve with full information of half the bits in the full key ($I_E = 0.5$). It introduces an error rate of 25% ($Q = 0.25$) into the key recieved by Bob. Using the assumptions given by (Csiszar and Korner, 1978) it can be shown that this means no secret key can be extracted. This is in fact true for all protocols.

Even in the case where Eve does not eavesdrop on all photons in the key, and instead on just a fraction p, then clearly $Q = p/4$ and so

$$I_E = p/2 = 2Q \tag{2.1}$$

Hence a secure key can only be extracted if $Q \geq 17\%$. The precise figure varies bypublication however.

2.1 Photon Number Splitting attack - PNS

In real world applications of QKD, the photon source is never a true strong single photon emitter. Typically a weak coherent pulse laser source is used. These sources emit pulses of coherent states, often containing 2 or more photons.

This presents a problem for the security of BB84 and B92, as described below.

2.1.1 BB84

The security weakness in coherent pulses comes from Eve's ability to nondestructively determine the number of photons in a pulse. The principle of the PNS attack is that Eve will block all single photon pulses, and for any pulse where multiple photons are detected, Eve will store in quantum memory a subset of the pulse, while allowing the rest to continue on to Bob (through an ideal quantum channel, to ensure his receipt of the photons). During the sifting phase, Alice and Bob's communications over the public channel can be used by Eve to construct a complete key from the stored states. The major benefit to Eve with this method is that it does not introduce an error in the states received by Bob; in fact, the only risk of detection comes from the losses due to single photon pulses being blocked.

As long as these losses do not reach a critical threshold (dependent on the length of the communication channel and the expected losses), Eve's actions remain undetected, and the security of the protocol is compromised.

2.1.2 B92

Against B92, the PNS attack is even more straightforward. No quantum memory is required; all that is sufficient is that Eve performs the same measurement as Bob, and blocks the message in the event of an inconclusive result. In this way, the losses are attributed to channel losses; as long as a critical threshold is not reached (as above), Eve will obtain full information of the key. Again, due to the lack of error in the received states, Eve will remain entirely unnoticed.