Our Setup, Bandwidth

1 Introduction

In this handout, we look again at our setup and characterise its capability to transmit or receive "secure" information. We will utilise the concept of "bandwidth": the amount of data that can be transmitted in a fixed amount of time, usually expressed in something-bit-per-second (i.e. bps, kbps, Mbps, or Gbps) or something-byte-per-second (i.e. Bps, kBps, MBps, or GBps). Note the difference in the capitalisation between bit vs. byte.

1.1 Public Channel

In our IR communication, each packet consists of 32 bits of data (4 ASCII characters), and requires around 300 ms for each packet transmission. Of those, $\sim$70 ms are used for transmitting the IR pulses (may vary depending on whether the messages have more 1s or 0s), while the rest of the time is for the computer-Arduino message transmission (both Alice and Bob) and some other overheads [1].

1.2 QKD Channel

In the QKD channel, each transmission cycle consists of 16 polarisation bits. Each bits requires 1.5 s to send, and the time is mostly wasted to rotate the polarisers ($\sim$1.1 s to rotate 90°). After the transmission cycle, the key sifting procedure is performed. On top of that, in BB84 scheme, in average only 50 percent of the bits will be kept (it ignores the bits where the polarisation bases do not match).

Right off the bat, you may have noticed that the key rate in the QKD channel is far lower than that in the classical communication. This is also true in the real world applications of QKD, but in a different way: the key rate is very low because the signal intensity drops over a long fibre. For a $\sim$50 km fibre, the signal drops $\sim$10 times. Thus, if one wants to build a QKD link between, say Singapore and Kuala Lumpur ($\sim$350 km), with the current technology, the key rate will drop by $\sim 10^7$ times.

[1] The value of $\sim$300 ms itself is determined by first, sending the packet with high repetition rate, and decreasing the rate until the packets do not drop unexpectedly. In our testing session, the rate is $\sim$5 Hz (corresponding to $\sim$200 ms). We add another $\sim$100 ms to be more on the cautious side: sometimes the computers slow down.

2 Assignment

Task 1 [2 pts] Estimate the bandwidth of the public channel!

Task 2 [2 pts] Suppose you want to send a 3-minute mp3 song with 196 kbps sound quality through our IR channel. How long will it take?

Task 3 [2 pts] Estimate the bandwidth of the QKD channel!
Note: Assume that the key sifting procedure takes $\sim$5 s.

Task 4 [2 pts] The public key cryptography infrastructure nowadays require at least key length of 1024 bits [2]. Suppose you also want to impose this criterion in this QKD system, how long will it take (in average) to produce the key?

Task 5 [2 pts] Find out about state-of-the-art bandwidth in classical channel and key generation rate in QKD! Comment on how our system compare with those system.

[2] https://en.wikipedia.org/wiki/Key_size