Solutions to Exercise Sheet 5

Dr Iain Styles

10 February 2008

1. The BB84 QKD Protocol Alice wishes to send Bob a message via a secure protocol. She chooses to use a private key encryption technique and decides to use the BB84 protocol to generate a provably secure private encryption key.

Alice's first step is to generate a random binary string. The string she generates is

$$b = 1010100010010111$$

Alice then encodes this as a string of quantum qubits as per the BB84 protocol, using the encoding HHHIIHIHHIIIHIIH. What is the quantum string that she generates?

Alice then sends the string to Bob, who decodes using IHHIHIHHIHIIIHIH. Alice and Bob annouce their encodings publicly and retain the qubits for which they chose the same encoding. What is the string that they retain?

Eve attempts to intercept the key distribution by measuring Alices quantum string before it reaches Bob. She decodes using IHIHIHIHHHIIHHIH; measures; and then re-encodes using the same choice. Which bits of Alice and Bob's retained string remain uncorrupted?

Solution:

To begin we apply Alice encoding to her classical string to generate a quantum string:

b:	`1010100010010111`
Encoding:	`HHHIIHIHHIIIHIIH`
$\mapsto \|q\rangle =$	`-+-01+1+-001+11-`

Bob then decodes $|q\rangle$ using his choice of encoding. He applies his chosen encoding to $|q\rangle$

	$\mapsto \|q\rangle =$	`-+-01+1+-001+11-`
and then measures:	Encoding:	`IHHIHIHHIHIIIHIH`
	Measure:	`?010???0??01??11`

Therefore the retained bit string is 01000111 (bits 2,3,4,8,11,12,15,16).

Let us now deal with Eve. Eve intercepts $|q\rangle$ and decode, measures and re-encodes using her choice of basis.

Alice b:	1010100010010111
Encoding:	HHHIIHIHHIIIHIIH
$\mapsto \|q\rangle =$	-+-01+1+-001+11-
Eve decodes using:	IHIHIHIHHHIIHHIH
getting:	-0-+10101+010-11
Eve measures:	?0??10101?010-11
and re-encodes:	±0±±10101±010±11

Eve's re-encoding gas changed the states of qubits 1,3,4,10,14. Comparing to the string Alice and Bob retained, Eve may have corrupted bits 3 and 4, leaving the uncorrupted string 100111.

2. Physical Realisations of Quantum Computers

Read chapter 7 of Nielsen and Chuang, especially sections 7.1, 7.2, 7.4, 7.6, 7.7. Aim to familiarise yourselves with the basic principles of each of the technologies outlined in the lectures, but don't worry too much about the details.