

# Quantum Computing and Cryptography

## Main paper 2010

Steve Vickers

March 3, 2010

### 1 Solutions

1 [LO2] (a) [10%]

(i)

$$\begin{aligned} |\psi\rangle &= \left( \frac{1}{\sqrt{6}}|0\rangle + \frac{1}{2\sqrt{3}}|1\rangle \right) |0\rangle + \left( -\frac{i}{\sqrt{3}}|0\rangle - \frac{\sqrt{5}}{2\sqrt{3}}|1\rangle \right) |1\rangle \\ &= \frac{1}{2} \left( \frac{\sqrt{2}}{\sqrt{3}}|0\rangle + \frac{1}{\sqrt{3}}|1\rangle \right) |0\rangle - \frac{\sqrt{3}}{2} \left( \frac{2i}{3}|0\rangle + \frac{\sqrt{5}}{3}|1\rangle \right) |1\rangle \end{aligned}$$

The probability of getting result 0 and 1 are  $\frac{1}{4}$  and  $\frac{3}{4}$  respectively.

(ii) If the result for Qbit 0 is 1, then the resulting state for Qbit 1 is  $\frac{2i}{3}|0\rangle + \frac{\sqrt{5}}{3}|1\rangle$ .

The probability of result 1 on Qbit 1 is now  $\frac{5}{9}$ .

(b) (i) [4%] By definition

$$C_{10}|xy\rangle = |x\rangle|y \oplus x\rangle$$

and so

$$C_{10}|x0\rangle = |x\rangle|0 \oplus x\rangle = |x\rangle|x\rangle.$$

[6%]  $|x\rangle$  is not a general state, but one of the two computational basis states  $|0\rangle$  and  $|1\rangle$ .  $C_{10}$  can clone these, but not superpositions of them.

$C_{10}$  does not clone  $H|0\rangle$ . We have

$$\begin{aligned} C_{10}(H|0\rangle \otimes |0\rangle) &= \frac{1}{\sqrt{2}}C_{10}(|00\rangle + |10\rangle) \\ &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ H|0\rangle \otimes H|0\rangle &= \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \\ &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle). \end{aligned}$$

(c) [10%]

$$C_{10}H_1|00\rangle = \frac{1}{\sqrt{2}}C_{10}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$C_{10}H_1|01\rangle = \frac{1}{\sqrt{2}}C_{10}(|01\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$C_{10}H_1|10\rangle = \frac{1}{\sqrt{2}}C_{10}(|00\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$C_{10}H_1|11\rangle = \frac{1}{\sqrt{2}}C_{10}(|01\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

The matrix is

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \end{pmatrix}$$

(d) [LO1] [10%] Quantum computation is likely to make it much easier to invert many one-way functions. Since many cryptographic protocols rely on it being hard to invert one-way functions (e.g. the problem of factoring large number for RSA), quantum computing will make it much easier to break those protocols. These include not only encryption but also protocols such as digital signatures. To some extent, though not all, quantum computing provides its own solutions to such problems. For example, quantum one-time pad makes it possible to use quantum channels to distribute one-time keys with detection of any eavesdropping.

2 [LO3]

(a) [LO4] [5%] The most usual technology at present generates a Qbit as a polarized photon, transmitted in fibre optic cable or even through air. The state of the Qbit is the polarization state (plane in some direction, or circular) of the photon. The main limitation is that they are very hard to store.

(b) [4%] Alice and Bob tell each other what types (1 or H) they used for preparing or measuring each Qbit.

(c) [5%] The useful Qbits were numbers 2, 3, 4, 5, 6, 7, 8, 11, 12, 16, 18, 20, 24, 25, 27.

The one-time pad has 15 bits. It is

100101010010101

(d) [5%] The sacrificed Qbits are numbers 2, 4, 6, 8, 12, 18, 24, 27. Bob must tell Alice what he measured for those Qbits (10000111) and Alice must tell Bob how she prepared them.

(e) [5%] Eight useful Qbits were sacrificed for interception checking. Suppose they were all intercepted, so there would be a probability of 25% for each Qbit that it gave the wrong measurement for Bob. Hence the probability of no discrepancies is  $(\frac{3}{4})^8 \approx 0.1$ . The seven non-sacrificed Qbits (the even numbered ones) give a one-time pad of

0111100

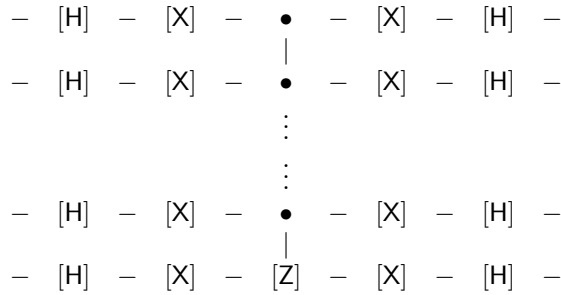
(f) [6%] If Eve intercepts more than 10% of the Qbits, then the probability that any given Qbit will show a discrepancy is at least  $\frac{1}{10} \times \frac{1}{4} = 0.025$ . The probability of no discrepancy in  $n$  check Qbits is  $0.975^n$ , so for 90% certainty we want  $0.975^n < 0.1$ , i.e.  $n \log 0.975 < -1$ . Since  $\log 0.975 \approx -0.01$ , this gives us  $n > 100$ . From the useful Qbits they need 100 for checking and 100 for the one-time pad, i.e. 200. Since on average only half the Qbits are useful, they need to use over 400 altogether.

3. [LO3]

(a) We have  $|\phi\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle)$ , so  $\langle a|\phi\rangle = \frac{1}{2}$ . Therefore, [4%]

$$\begin{aligned} \mathbf{WV}|\phi\rangle &= \mathbf{W}(|\phi\rangle - 2\langle a|\phi\rangle|a\rangle) = \mathbf{W}|\phi\rangle - \mathbf{W}|a\rangle \\ &= |\phi\rangle - 2\langle\phi|a\rangle|\phi\rangle + |a\rangle = |a\rangle. \end{aligned}$$

(b) The right hand side of this reverses the sign if all the Qbit states are  $|0\rangle$ . This is the multi-controlled Z gate, but with the roles of 0 and 1 reversed for every Qbit. Hence  $-\mathbf{W}$  is got by putting Hs and Xs on both sides on every line. [6%]



(c)  $\mathbf{V}|a_{\perp}\rangle = |a_{\perp}\rangle - 2\langle a|a_{\perp}\rangle|a\rangle = |a_{\perp}\rangle$ , and  $\mathbf{W}$  takes  $|a_{\perp}\rangle$  to its reflection in  $|\phi\rangle$ , an angle  $2\theta$  away. Since  $\mathbf{WV}$  rotates  $|a_{\perp}\rangle$  an angle  $2\theta$ , it does the same for all the vectors.

$\theta$  is  $\frac{\pi}{2}$  less the angle between  $|a\rangle$  and  $|\phi\rangle$ , which are unit vectors,  $\sin\theta$  is the cosine of the angle between  $|a\rangle$  and  $|\phi\rangle$  which is  $\langle a|\phi\rangle = \frac{1}{2^{n/2}}$ . If  $n$  is large then  $\theta$  is small and so  $\theta \approx \sin\theta = \frac{1}{2^{n/2}}$ . To rotate  $|\phi\rangle$  to  $|a\rangle$  is through an angle  $\frac{\pi}{2} - \theta$ , so we need  $2k\theta \approx \frac{\pi}{2} - \theta$ . We therefore take  $k$  to be the integer closest to  $\frac{\pi/2}{2\theta} \approx \frac{\pi}{4} 2^{n/2}$ . [10%]

(d) We have

$$\begin{aligned} \mathbf{U}_f|x\rangle_n \mathbf{H}|1\rangle &= (-1)^{f(x)}|x\rangle \mathbf{H}|1\rangle \\ &= \mathbf{V}|x\rangle \mathbf{H}|1\rangle. \end{aligned}$$

Hence if prepare the output Qbit as  $\mathbf{H}|1\rangle$  we can calculate  $\mathbf{V}$  on the input Qbits by applying  $\mathbf{U}_f$  to all of them. We can also compute  $\mathbf{W}$  using a circuit as described in part (b). Then applying  $\mathbf{WV}$  to  $|\phi\rangle$   $k$  times we obtain a state close to  $|a\rangle$  and we can, with high probability, find  $a$  by measuring the state. [10%]

4. [LO3]

(a) We apply  $U_{FT}$  to  $|\psi\rangle$  and then measure the state. The theory shows that there is a better than 0.4 probability that the result  $y$  will be within  $\frac{1}{2}$  of  $\frac{j2^n}{r}$  for some integer  $j$ , and that in that case the following process will find the value of  $\frac{j}{r}$ . (However, if we are unlucky and  $j$  and  $r$  have large factors in common, we shall still not find  $j$  and  $r$ .) We apply the continued fraction process to  $\frac{y}{2^n}$  to try to find a rational approximation  $\frac{j'}{r'}$  to  $\frac{y}{2^n}$  with denominator  $r' < 2^{n/2}$ . This is likely to be  $\frac{j}{r}$  reduced to lowest terms, so we check whether small multiples  $r'$ ,  $2r'$  etc. are the period. If none of them is, then we have to try again with another  $|\psi\rangle$ . [10%]

(b)

(i)  $m = 3$ , since  $m = 4$  gives  $x_0 + (m - 1)r = 1 + 3 \times 3 = 10 \geq 8 = 2^n$ . [3%]

(ii)  $y = 0$ : When the result is 0, no information can be found about  $r$  so we just have to try again with a new  $|\psi\rangle$ . [3%]

(iii)  $y = 5$ : [10%]

In this case we use the continued fractions and find

$$\frac{5}{8} = \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}$$

Neglecting the final  $\frac{1}{2}$ , we get

$$\frac{1}{1 + \frac{1}{1 + \frac{1}{1}}} = \frac{1}{1 + \frac{1}{2}} = \frac{2}{3}$$

and so we check for whether the denominator 3 is a period – which it is. (Otherwise we would try small multiples: say 6, 9, 12, 15. If that still doesn't work, we try another  $|\psi\rangle$ ).

(iv)  $y = 6$ : [4%]

In this case, continued fractions give

$$\frac{6}{8} = \frac{3}{4} = \frac{1}{1 + \frac{1}{3}}$$

There are no shorter continued fractions, so we check whether 4 is a period. It is not, so we try another  $|\psi\rangle$ .