Quantum cryptology and Security

Mid-Semester Examination

Tufan Singha Mahabatra
CRS2014.

1 (a) we suppose that Alice is measuring using the orthonormal basis $\{|a_0\rangle, |a_1\rangle\}$ and Bob is measuring with orthonormal basis $\{|b_0\rangle, |b_1\rangle\}$. A typical qubit for Alice is $|v\rangle = c_0|a_0\rangle + c_1|a_1\rangle$ & for Bob it is $|w\rangle = d_0|b_0\rangle + d_1|b_1\rangle$

Now, $|v\rangle \otimes |w\rangle = (c_0|a_0\rangle + c_1|a_1\rangle) \otimes (d_0|b_0\rangle + d_1|b_1\rangle)$

$= c_0d_0|a_0b_0\rangle + c_0d_1|a_0b_1\rangle + c_1d_0|a_1b_0\rangle + c_1d_1|a_1b_1\rangle$.

Let $r = c_0d_0$, $s = c_0d_1$, $t = c_1d_0$, $u = c_1d_1$. So,

$|vw\rangle = r|a_0b_0\rangle + s|a_0b_1\rangle + t|a_1b_0\rangle + u|a_1b_1\rangle$.

and as, $|vw\rangle$ is also a qubit so,

$$r^2 + s^2 + t^2 + u^2 = 1.$$

and $ru = c_0d_0c_1d_1 = c_0d_1d_0c_1 = st$.

Now, if we are given any tensor of the form $r|a_0b_0\rangle + s|a_0b_1\rangle + t|a_1b_0\rangle + u|a_1b_1\rangle$ with $r^2 + s^2 + u^2 + t^2 = 1$ there are two case.

Case-(i) if $ru = st$ in this case we say that, Alice's and Bob's qubit's are not entangled.

Case-(ii) if $ru \neq st$ then we say that, Alice's and Bob's qubits are entangled.

So, for an entanglemet state we can't write this state as a tensor product of two states.

1 (b) Let $|\psi\rangle = \frac{1}{\sqrt{2}}\left(\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n} + \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)^{\otimes n}\right)$

Now, $H^{\otimes n}|\psi\rangle = \frac{1}{\sqrt{2}} H^{\otimes n}\left[\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n} + \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)^{\otimes n}\right]$

$= \frac{1}{\sqrt{2}}\left[H^{\otimes n}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n} + H^{\otimes n}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)^{\otimes n}\right]$

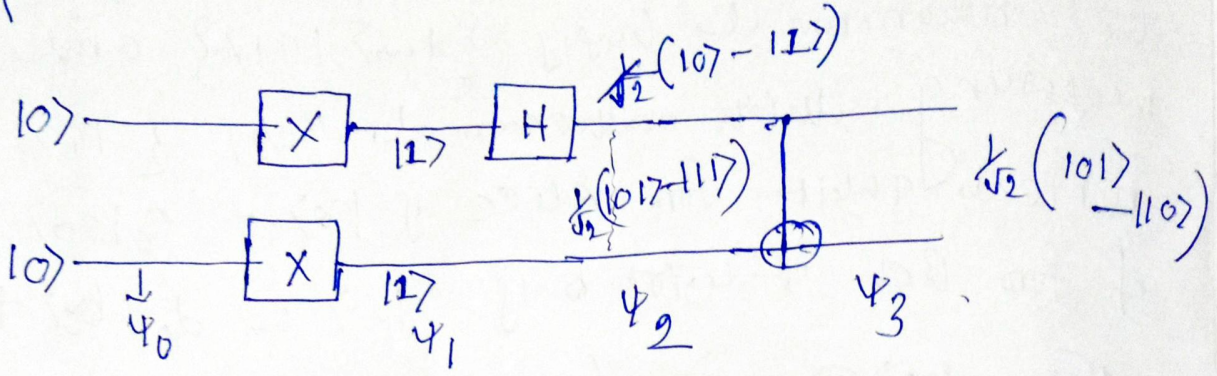
as $H^{\otimes n}$ is linear

$= \frac{1}{\sqrt{2}}\left[|0^n\rangle + |1^n\rangle\right]$.

As $\frac{1}{\sqrt{2}}\left(|0^n\rangle + |1^n\rangle\right)$ is an entangled in $\{|0\rangle, |1\rangle\}$ basis.

and $H^{\otimes n}$ is an unitary transformation and we know that, entanglement is same if we change our basis so, $|\psi\rangle$ is also an entangled state.

2@



here X is X gate i.e, $X|0\rangle = |1\rangle$
$X|1\rangle = |0\rangle$.

(b) & H is Hadamard gate.

$H|0\rangle = |+\rangle$ & $H|1\rangle = |-\rangle$

& $C_{NOT}|x,y\rangle = |x, x \oplus y\rangle$.

(c) here $\Psi_0 = |00\rangle$,
$\Psi_1 = |11\rangle$ & $\Psi_2 = \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle)$.
$\Psi_3 = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

(b) we know that matrix rep of X is —

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \& \quad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

$$\& \; C_{NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix}.$$

Now, the 4×4 matrix will be —

Composition of matrix

$= (\quad) \; C_{NOT} \circ (\quad)(H \otimes I) \circ (X \otimes X) = M_{4\times 4}$ (say)

$X \otimes X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$= \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & X \\ X & 0 \end{pmatrix}$.

$H \otimes I = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

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

$= \frac{1}{\sqrt{2}} \begin{pmatrix} I & I \\ I & -I \end{pmatrix}$, $C_{NOT} = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix}$

$$M_{4\times4} = C_{NOT} \circ (H \otimes I) \circ (X \otimes X)$$

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

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

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} X & X \\ -X^2 & X^2 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} X & X \\ -I & I \end{pmatrix}$$

$\because X^2 = I$.

$$\therefore M_{4\times4} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}.$$

(5) Let $|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ & $|\psi^\perp\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$

& we know that Hadamard gate H is defined by matrix $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. and it is given that —

$$H(|\psi\rangle) = \frac{1}{\sqrt{2}} (|\psi\rangle + |\psi^\perp\rangle).$$

$$\Rightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} a+c \\ b+d \end{pmatrix}.$$

$$\Rightarrow \begin{pmatrix} a+b \\ a-b \end{pmatrix} = \begin{pmatrix} a+c \\ b+d \end{pmatrix} \Rightarrow \begin{matrix} b=c \\ \& \; a-b=b+d \end{matrix}.$$

also given that —

$$H(|\psi^\perp\rangle) = \frac{1}{\sqrt{2}} (|\psi\rangle - |\psi^\perp\rangle)$$

$$\Rightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} a-c \\ b-d \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} c+d \\ c-d \end{pmatrix} = \begin{pmatrix} a-c \\ b-d \end{pmatrix}.$$

$\Rightarrow c = b$ & $c + d = a - c$

So, combining both we get —

$b = c$ & $a = 2c + d \Rightarrow d = a - 2b$,

~~Again~~ as, $\psi^{\perp} = \begin{pmatrix} c \\ d \end{pmatrix}$ & and $\psi^{\perp}$ is orthogonal to ψ So, $\left\langle \begin{pmatrix} a \\ b \end{pmatrix} \middle| \begin{pmatrix} c \\ d \end{pmatrix} \right\rangle = 0$

$\Rightarrow \quad a\bar{c} + b\bar{d} = 0$.

$\Rightarrow (2c + d)\bar{c} + c\bar{d} = 0$ as $b = c$

$\Rightarrow \quad 2c\bar{c} + d\bar{c} + c\bar{d} = 0$ & $a = 2c + d$

here if $|\psi\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \Rightarrow a = 0, b = 0$.

$|\psi^{\perp}\rangle = |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \Rightarrow \begin{matrix} c = 0 \\ d = 1 \end{matrix}$.

which satisfies $b = c$ & $a = 2c + d$.

But if $|\psi\rangle = |0\rangle \Rightarrow a = 1, b = 0$

$|\psi^{\perp}\rangle = i|1\rangle \Rightarrow c = 0, d = i$

here $b = c$ But $2c + d = i \neq a = 1$.

So, it not satisfy the condition.

~~So, it not satisfies~~

Now, $|\psi\rangle = a|0\rangle + b|1\rangle$

& $|\psi^{\perp}\rangle = b|0\rangle + (a - 2b)|1\rangle$

as $c = b$ & $d = a - 2b$.

Now, here $|a|^2 + |b|^2 = 1$ & $|b|^2 + |a - 2b|^2 = 1$

So, $|b|^2 + |a|^2 + 4|b|^2 - 2\bar{a}b - 2a\bar{b} = 1$

$\Rightarrow 2|b|^2 = \bar{a}b + a\bar{b}$ ... — (1)

Also, we have

$$2c\bar{c} + d\bar{c} + \bar{d}c = 0$$

here $c = b$ & $d = (a - 2b)$.

$$\Rightarrow 2b\bar{b} + (a-2b)\bar{b} + (\bar{a} - 2\bar{b})b = 0$$

$$\Rightarrow 2b\bar{b} + a\bar{b} - 2b\bar{b} + \bar{a}b - 2b\bar{b} = 0$$

$$\Rightarrow 2b\bar{b} = a\bar{b} + \bar{a}b \quad \text{——— (2)}$$

from (1) & (2) we get $2|b|^2 = a\bar{b} + \bar{a}b$.

$\Rightarrow |b|^2 = 0 \Rightarrow b = 0 = c$

So, $\psi = \begin{pmatrix} a \\ b \end{pmatrix}$ s.t. $2|b|^2 = a\bar{b} + \bar{a}b$.

(4) (a) Problem statement of Deutsch-Jozsa algorithm

Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function which has a promise that it can be either balanced or constant function. Now, if we are able to know the output of f, after giving some input, we have to find f is balanced or constant.

By Deutsch-Jozsa Algorithm we can able to find either f is balanced or constant in a single query.

(b) In classical,

first we will check the half of the input values i.e, $\frac{2^n}{2} + 1 = 2^{n-1}$ values.

If we get all of the 2^{n-1} value output same then if we check one more value & also if it gives the same output it can't be a balance function $\Rightarrow$ f is constant function as promised before.

If f doesn't give the same value f is balanced.

So, in $2^{n-1} + 1$ query we can determine whether f is constant or balanced in classical query.

But in Deutsch-Jozsa algorithm, in a single query we can able to give the same answer.

So, in classical we need $2^{n-1} + 1$ query & in quantum we need 1 query.

(c) $f: \{0,1\}^3 \longrightarrow \{0,1\}$ given by —

$$f(x_1, x_2, x_3) = x_1 x_2 \oplus x_2 x_3 \oplus x_1 x_3$$

In Deutsch-Jozsa before the measurement step.

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x \cdot z \oplus f(x)}}{2^3} |z\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$= \frac{1}{2^n} \sum_z \sum_x w_f(z) |z\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

3) $|\psi_3\rangle = \left(\sum_{z \in \{0,1\}^3} \frac{W_f(z)}{2^3} |z\rangle \right) |-\rangle$

Now, $W_f(z) = \sum_{x \in \{0,1\}^3} (-1)^{f(x) \oplus x \cdot z}$

$f(x_1,x_2,x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3$.

$f(0,0,0) = 0$	$W_f(000) = 0$
$f(001) = 0$	$W_f(001) = 4$
$f(010) = 0$	$W_f(010) = 4$
$f(011) = 1$	$\Rightarrow W_f(011) = 0$
$f(100) = 0$	$W_f(101) = 0$
$f(101) = 1$	$W_f(110) = 0$
$f(110) = 1$	$W_f(111) = -4$.
$f(111) = 1$	$W_f(100) = 4$

3) b. $|\psi_3\rangle = \frac{1}{8} \sum_z$

$= \frac{1}{8} \Big(\sum_z \big(1 + (-1)^{z_1} + (-1)^{z_2} + (-1)^{z_3} + (-1)^{z_1+z_2+1} + (-1)^{z_1+z_3+1} + (-1)^{z_2+z_3+1} + (-1)^{z_1+z_2+z_3+1} \big) |z\rangle \Big) |-\rangle$

$= \frac{1}{8} \Big(4|001\rangle + 4|010\rangle + 4|100\rangle - 4|111\rangle \Big) |-\rangle$

$= \frac{1}{2\sqrt{2}} \Big(|001\rangle + |010\rangle + |100\rangle - |111\rangle \Big) \otimes (|0\rangle - |1\rangle)$

1 (b) Let $|\psi\rangle = \frac{1}{\sqrt{2}}\left(\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n} + \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)^{\otimes n}\right)$

Now, $H^{\otimes n}|\psi\rangle = \frac{1}{\sqrt{2}} H^{\otimes n}\left[\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n} + \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)^{\otimes n}\right]$

$= \frac{1}{\sqrt{2}}\left[H^{\otimes n}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n} + H^{\otimes n}\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)^{\otimes n}\right]$

as $H^{\otimes n}$ is linear

$= \frac{1}{\sqrt{2}}\left[|0^n\rangle + |1^n\rangle\right]$.

As $\frac{1}{\sqrt{2}}\left(|0^n\rangle + |1^n\rangle\right)$ is an entangled in $\{|0\rangle, |1\rangle\}$ basis.

and $H^{\otimes n}$ is an unitary transformation and we know that, entanglement is same if we change our basis so, $|\psi\rangle$ is also an entangled state.

(3) (a) $x \cdot y = 0$ for 00, 10, 01

& $x \cdot y = 1$ for 11.

$\therefore P(x \cdot y = 0) = 3/4$ & $P(x \cdot y = 1) = 1/4$.

So, in classical the best strategy for A, B could be just output 0 always.

i.e, $a \oplus b = 0$ i.e $a = 0, b = 0$.

because this way they have 75% chance of winning the game.

(b) Let A, B shares an entangled pair say $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Let A has the first qubit of the pair and B has the second one.

They receive random (x, y) inputs.

Game strategy:-

for A if $x=0$ A do nothing

$x=1$ A Rotate their qubit by $\pi/8$.

Measure their qubit and output the value a.

for B

If $y=0$ do nothing

if $y=1$ Rotate their qubit by $-\pi/8$.

Measure their qubit and output value b,

So,

If $x=y=0 \Rightarrow$ They both do nothing

Measuring they get $ab=00$ or $ab=11$

$\Rightarrow a=b$.

Say $a \oplus b = 0 \Rightarrow$ They win with probability 1.

If $x=0, y=1$ A doesn't Rotate

$\Rightarrow$ gets classical bit a

B rotates by $-\pi/8$.

⇒ If $a=0$ ⇒ B's qubit becomes —

$\cos\pi/8\,|0\rangle - \sin\pi/8\,|1\rangle$.

Measuring $P(b=0) = \cos^2\pi/8$,

$P(b=1) = \sin^2\pi/8$.

$Pr(win) = \cos^2\pi/8$. $(a=0, b=0)$

If $a=1$ ⇒ B's qubit → becomes,

$\sin\pi/8\,|0\rangle + \cos\pi/8\,|1\rangle$

⇒ $Pr(b=1) = \cos^2\pi/8$, $Pr(b=0) = \sin^2\pi/8$.

$P(win) = \cos^2\pi/8$ $(a=1, b=1)$

∴ overall win $= \frac{1}{2}\cos^2(\pi/8) + \frac{1}{2}\cos^2(\pi/8)$

$= \cos^2\pi/8$.

If $x=1, y=0$ similar case.

If $x=1, y=1$ ⇒ both parties.

⇒ chances of both measuring diff and classical bits ⇒ i.e. $|01\rangle, |10\rangle \Rightarrow 1/2$

$P(win) = \frac{1}{4}\cdot 1 + \frac{1}{4}\cdot\cos^2\pi/8 + \frac{1}{4}\cos^2\pi/8 + \frac{1}{4}\cdot\frac{1}{2}$

≈ 0.80

∴ $P(win) = 80 > P(win)$ in classical setting.

75%.

6 (a) (7) (a) Given a function (implemented by a black box or oracle) $f: \{0,1\}^n \to \{0,1\}^n$, with promise that for a unknown $s \in \{0,1\}^n$, for all $x, y \in \{0,1\}^n$,

$f(x) = f(y)$ iff $x = y$ or $y = x \oplus s$.

The goal is to identify s by making as few queries to $f(x)$ as possible.

(b) The given truth table is —

x	$f(x)$
000	110
001	101
010	000
011	011
100	101
101	110
110	011
111	000

here $f(010) = f(111) = 000$

let $x = 010$, $y = 111$ But $x \neq y$.

$\Rightarrow s = x \oplus y$

$= 010 \oplus 111$

$= 101$

$\Rightarrow s = 101$ ..

since $f(000) = f(101) = 110$

also, $S = 000 \oplus 101 = 101$

Also $f(011) = f(110) = 011$

$\Rightarrow 011 \oplus 110 = 101 = S$

& $f(001) = f(100) = 101$

$\Rightarrow 001 \oplus 100 = 101 = S$..

6(a) Let $E : K \times M \to C$ be a encryption

Let $K = \{0,1\}^n$.

Let A be a key-recovery adversary for E.

Let k be a secret number.

$Pr(A \text{ win}) = Pr(\hat{K} = k)$ if A outputs $\hat{K}$.

$= 1/2^n$.

in Grovers search alg if $\theta \to 0$ so,

$\sin\theta \approx \theta$.

$\Rightarrow (2t+1)\theta \approx \pi/2$

$\Rightarrow t \approx \left(\frac{\pi}{2\theta} - 1\right) 1/2$

$\approx \frac{\pi}{4\theta}$

and θ for $\sin^2\theta = \theta^2 \approx 1/2^n$

$\Rightarrow \theta \approx 1/2^{n/2}$

$\therefore t \approx \frac{\pi}{2\theta} = \pi/4\, 2^{n/2} = O(2^{n/2})$

So, effective key length is $\frac{n}{2}$ if adversary A use Grover's search algorithm.

6 (b)

x_1 x_2 x_3	$f(x_1, x_2, x_3)$
0 0 0	1
0 0 1	1
0 1 0	1
0 1 1	0
1 0 0	1
1 0 1	1
1 1 0	1
1 1 1	1

let $g(x,y,z) = 1 \oplus f(x,y,z)$

$S = \{(x_1, x_2, x_3) \mid f(x_1, x_2, x_3) = 0\}$

$= \{(x_1, x_2, x_3) \mid g(x_1, x_2, x_3) = 1\}$

$P(\text{good term for } g) = \frac{1}{23}$.

$\Rightarrow \sqrt{23} =$

So, apply Grover algorithm 3 times to find the good term.

S set.