

# QUANTUM INFORMATION

## HW 5



AMIT LEVI 207422650

GILAD LEVI

1)A)

$$\phi = \frac{1}{\sqrt{N}}, W = \sin - \frac{2\sqrt{N-1}}{N}$$

$$\rightarrow \Pr(\beta) = \frac{1}{2}(1 - \cos(2\omega n + 2\phi))$$

$$\text{For } N=4 \rightarrow \phi = \frac{1}{2}, \omega = \sin\left(\frac{\sqrt{3}}{2}\right) = \frac{\pi}{3}$$

$$\rightarrow P_r(\beta) \approx \frac{1}{2}(1 - \cos\left(\frac{2\pi}{3} + 1\right)) \approx 1$$

## 1. B

In a classical algorithm, we will need 3 calls to the Oracle in the worst case because the probability of finding the target element on the first two calls is less than 50%. Therefore, we need to make at least three calls to the Oracle to ensure that we have a greater than 50% chance of finding the target element. In the average case, we will need 2.25 calls because the probability of finding the target element on each call is  $1/4$ . Therefore, the expected number of calls is  $1/4 + 2/4 + 3/4 = 2.25$ .

1)c)

$$|\varphi\rangle \rightarrow A(2|00\rangle\langle 00| - I) \cdot |\varphi\rangle = 2 \begin{pmatrix} |\varphi\rangle \\ 0 \\ 0 \\ 0 \end{pmatrix}$$



the truth table

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \xrightarrow{A} \begin{pmatrix} 2 \\ 0 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle$$

$$|01\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \xrightarrow{A} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |00\rangle$$

$$|10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \xrightarrow{A} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ -1 \\ 0 \end{pmatrix} = -|10\rangle$$

$$|01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \xrightarrow{A} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \\ 0 \\ 0 \end{pmatrix} = -|01\rangle$$

$$|00\rangle \xrightarrow{IH, CNOT} \frac{1}{\sqrt{2}} |1\rangle |1\rangle - \frac{1}{\sqrt{2}} |1\rangle |0\rangle = -|1\rangle |-\rangle \xrightarrow{IH, xx} -|00\rangle$$

$$|01\rangle \xrightarrow{IH, CNOT} \frac{1}{\sqrt{2}} |1\rangle |1\rangle + \frac{1}{\sqrt{2}} |1\rangle |0\rangle = |1\rangle |+\rangle \xrightarrow{IH, xx} |01\rangle$$

$$|10\rangle \xrightarrow{IH, CNOT} \frac{1}{\sqrt{2}} |0\rangle |0\rangle - \frac{1}{\sqrt{2}} |0\rangle |1\rangle = |0\rangle |-\rangle \xrightarrow{IH, xx} |10\rangle$$

$$|11\rangle \xrightarrow{IH, CNOT} \frac{1}{\sqrt{2}} |0\rangle |0\rangle + \frac{1}{\sqrt{2}} |0\rangle |1\rangle = |0\rangle |+\rangle \xrightarrow{IH, xx} |11\rangle$$

The truth tables is the same (A and g.p-1)

$$1)d) \quad 1)C) \rightarrow A|\varphi\rangle = 2 \begin{pmatrix} |\varphi\rangle \\ 0 \\ 0 \\ 0 \end{pmatrix} - |\varphi\rangle$$

$$For \rightarrow |b\rangle = (H \otimes H) |B\rangle \in \{+, -\}^2 \rightarrow |b\rangle_0 = \frac{1}{2}$$

$$A|b\rangle = 2 \begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \\ 0 \end{pmatrix} - |b\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} - |b\rangle = |00\rangle - |b\rangle$$

1)f)

$$|001\rangle \rightarrow_{HHH} |++-\rangle \Rightarrow_{V_f} \frac{1}{2} \sum_x [|x\rangle (-1)^{f(|x\rangle)} |-\rangle] =$$

$$\frac{1}{2} \left( |00\rangle (-1)^{f(|00\rangle)} |-\rangle + |01\rangle (-1)^{f(|01\rangle)} |-\rangle + |10\rangle (-1)^{f(|10\rangle)} |-\rangle + |11\rangle (-1)^{f(|11\rangle)} |-\rangle \right) \rightarrow_{HHI}$$

$$\frac{1}{2} \left( (|00\rangle - |++\rangle) (-1)^{f(|00\rangle)} |-\rangle + (|00\rangle - |+-\rangle) (-1)^{f(|01\rangle)} |-\rangle + (|00\rangle - |-+\rangle) (-1)^{f(|10\rangle)} |-\rangle + (|00\rangle - |--\rangle) (-1)^{f(|11\rangle)} |-\rangle \right) \rightarrow_{HHH}$$

$$\frac{1}{2} \left( (|++\rangle - |00\rangle) (-1)^{f(|00\rangle)} |1\rangle + (|++\rangle - |01\rangle) (-1)^{f(|01\rangle)} |1\rangle + (|++\rangle - |10\rangle) (-1)^{f(|10\rangle)} |1\rangle + (|++\rangle - |11\rangle) (-1)^{f(|11\rangle)} |1\rangle \right) = \frac{1}{2} \sum_x [|++\rangle - |x\rangle (-1)^{f(|x\rangle)} |1\rangle]$$

$$= \frac{1}{2} \left( \sum_{x \neq \beta} [|++\rangle - |x\rangle (-1)^{f(|x\rangle)} |1\rangle] + [|++\rangle - |\beta\rangle (-1)^{f(|\beta\rangle)} |1\rangle] \right)$$

$$= \frac{1}{2} \left( \sum_{x \neq \beta} [|++\rangle - |x\rangle] |1\rangle - [|++\rangle - |\beta\rangle] |1\rangle \right)$$

$$= \frac{1}{2} \left( \sum_{x \neq \beta} [|++\rangle - |x\rangle] - [|++\rangle - |\beta\rangle] \right) |1\rangle = \frac{1}{2} \left( 2|++\rangle - \sum_{x \neq \beta} |x\rangle + |\beta\rangle \right) |1\rangle$$

$$= \frac{1}{2} \left( \sum_x |x\rangle - \sum_{x \neq \beta} |x\rangle + |\beta\rangle \right) |1\rangle = \frac{1}{2} 2|\beta\rangle |1\rangle = |\beta\rangle |1\rangle$$

## 2. A

Alice ,Golda and Bob will send to David  $x_1 x_2 x_3$  , David will calculate the sum of  $x_i$  and cheack if  $S$  equal to zero mod 4 ,in this protocol there is transfer of 6 bits.


## 2. B

$S_3 = x_4 + x_2 + x_1$  , according  $S_3 + x_3 = S = 0 \text{ mod } 2$  ,

Additionally the  $\text{lsb}(S_3 + x_3) = 0$

So thats means  $\text{lsb}(x_3) [+] \text{lsb}(S_3) = 0$  so  $\rightarrow \text{lsb}(x_3) = \text{lsb}(S_3)$

There for to know the valus of  $x_3$  we can just find the value of  $S_3$ .

Lets optimize the protocol with that Bob and Alice will send  $x_1$  and  $x_2$  and Golda will send the msg( $x_3$ ) .

David just have now to sum the elements  $x_i$  and check if  $\text{msg}(x_3) = 0 \text{ mod } 4$ ,so in this protocol only 5 bits is needed to be transferred.

## 2. C

$p_i$  is the participant of the number  $i$ ,lets extand the protocol linke in clause number 2 for the participants :

$p_1, p_2, p_3, \dots, p_{N-2}$  of the numbers  $x_1, x_2, x_3, \dots, x_{N-2}$

to  $p_N$  send the msg( $x_{N-1}$ ) by  $p_{N-1}$ .

$p_N$  calculating  $S_{N-1}$  , the lsb of  $x_{N-1}$  is known and with the msg of  $x_{N-1}$  we know what is  $x_{N-1}$  now we can calculate if  $S = 0 \text{ mod } 4$  in this protocol  $2 \cdot N - 3$  bits was transferred.

## 2.D

Alice, Golda and Bob will send to David  $x_1, x_2, x_3$ , David will calculate the sum of  $x_i$  and check if  $S$  equal to zero mod 4, in this protocol there is transfer of 6 bits.

## 2.E

The state of the system after applying the gates  $U_1, U_2, U_3$ , and  $U_4$  to the initial state  $|0\rangle$  is represented by the situation  $|+U_4U_3U_2U_1$ . This situation can be written mathematically as:

$$|\psi\rangle = U_4U_3U_2U_1|0\rangle$$

Each of the gates  $U_1, U_2, U_3$ , and  $U_4$  may depend on the values of  $x_1, x_2, x_3$ , and  $x_4$ . For example, if  $U_1 = e^{(i\pi x_1)}$ , then the state of the system after applying  $U_1$  will depend on the value of  $x_1$ .

Similarly, if  $U_2 = e^{(i\pi x_2)}$ , then the state of the system after applying  $U_2$  will depend on the value of  $x_2$ , and so on.

Therefore, the state of the system after applying these gates,  $|\psi\rangle$ , may contain information about the values of  $x_1, x_2, x_3$ , and  $x_4$ . By measuring the state of the system, we may be able to extract this information.


This is useful in constructing a quantum protocol to solve the given problem, as we are trying to determine whether  $S$  is divisible by 4 without a remainder. This depends on the values of  $x_1, x_2, x_3$ , and  $x_4$ , which are encoded in the state of the system after applying the gates  $U_1, U_2, U_3$ , and  $U_4$ .

So the situation  $|+U_4U_3U_2U_1$  is worth considering because it represents the state of the system after applying these gates, which may contain information about the values of  $x_1, x_2, x_3$ , and  $x_4$  that we need to solve the given problem.



## 2.F

1. A quantum protocol that solves the given problem with probability 1 with three qubits could involve the following steps:
  - Alice applies the  $U_1$  gate to her qubit and sends it to Bob.
  - Bob applies the  $U_2$  gate to his qubit and the qubit received from Alice, and sends the resulting qubit to Golda.
  - Golda applies the  $U_3$  gate to her qubit and the qubit received from Bob, and sends the resulting qubit to David.
  - David applies the  $U_4$  gate to his qubit and the qubit received from Golda, and measures the resulting state.

If the measurement result is  $|0\rangle$ , then  $4 \bmod 0 \equiv S$ . If the measurement result is  $|1\rangle$ , then  $4 \bmod 0 \neq S$ . 

1. To generalize the quantum protocol to  $N$  participants, we can follow the same steps as before, but with each participant applying their respective  $U_i$  gate to their qubit and the qubit received from the previous participant, and sending the resulting qubit to the next participant in the chain until it reaches the final participant. The number of qubits transmitted in this case will be  $N-1$ .




## 2.6

To generalize the quantum protocol to  $N$  participants, we can follow the same steps as before, but with each participant applying their respective  $U_i$  gate to their qubit and the qubit received from the previous participant. This can be represented mathematically as follows:

Alice applies the  $U_1$  gate to her qubit and sends it to Bob:

$$|\psi\rangle = U_1|0\rangle$$

Bob applies the  $U_2$  gate to his qubit and the qubit received from Alice, and sends the resulting qubit to Golda:  $|\psi\rangle = U_2(|0\rangle \otimes |\psi\rangle)$  

Golda applies the  $U_3$  gate to her qubit and the qubit received from Bob, and sends the resulting qubit to David:  $|\psi\rangle = U_3(|0\rangle \otimes |\psi\rangle)$

David applies the  $U_4$  gate to his qubit and the qubit received from Golda:  $|\psi\rangle = U_4(|0\rangle \otimes |\psi\rangle)$

Where  $|\psi\rangle$  represents the state of the system after each participant applies their respective gate.

The number of qubits transmitted in this case will be  $N-1$ , because each participant except for the first and last participant sends one qubit to the next participant in the chain.

### שאלה 3:

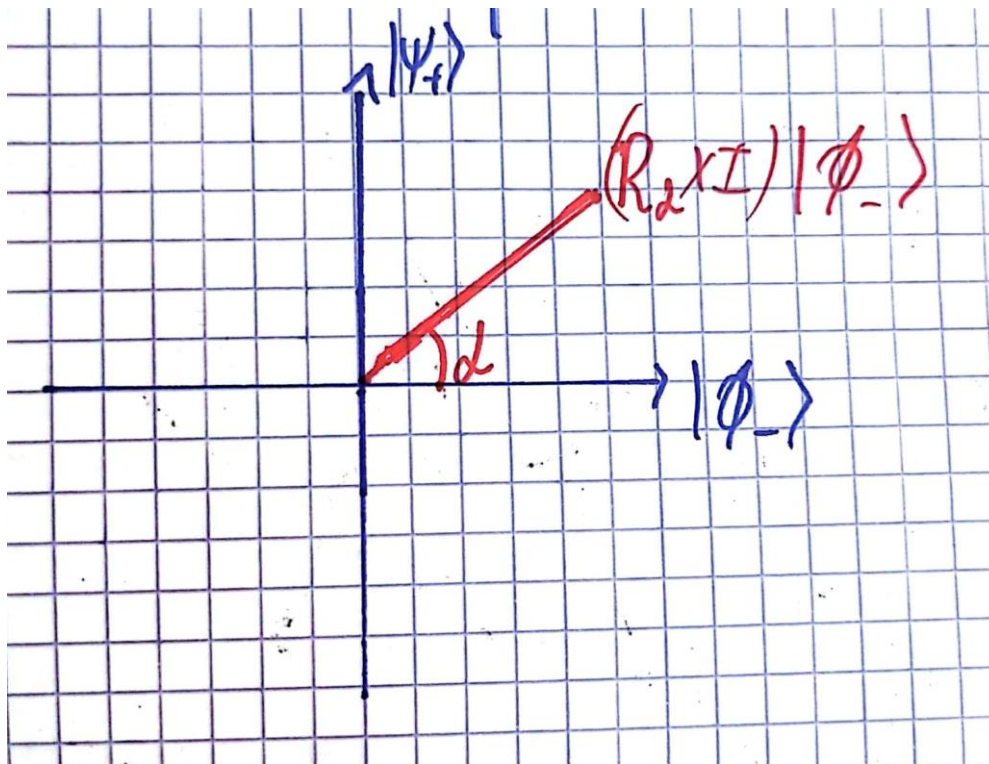
#### סעיף 3.1:

בגלל שכל הפעולות הן מקומיות, אליס ובוב יכולים להחליט מה יהיה הפלט שלהם בהנתן רק הביט שכל אחד מהם מקבל. אראה שלכל בחירה של פלטים עבור 2 האפשרויות לכל קלט קיימת בחירה של  $x_a, x_b$  שעבורה הם טועים ומכיוון שיש רק 4 אפשרויות, ההסתברות לפתרון תהיה לכל היותר  $\frac{3}{4}$ . כדי שאליס ובוב לא יטעו על הקלט 01 הם צריכים תוצאה סופית 0, כלומר לבחור את אותו ביט. כל הפעולות הן XOR ולכן אניח בה"כ כי שניהם בחרו 0. כעת, כדי שלא יטעו על הקלט 10 הם שוב צריכים לבחור את אותו ביט. אם שניהם בחרו שוב 0, אז עבור הקלט 11 נקבל תוצאה 0 כאשר צריך 1 ואם שניהם בחרו 1 אז עבור הקלט 00 נקבל תוצאה 1 כשצריך 0.

#### סעיף 3.2:

$$R_\alpha \otimes I |\phi_-\rangle = \frac{(R_\alpha |0\rangle)|0\rangle - (R_\alpha |1\rangle)|1\rangle}{\sqrt{2}} = \frac{\begin{pmatrix} \cos \alpha \\ \sin \alpha \end{pmatrix} |0\rangle - \begin{pmatrix} -\sin \alpha \\ \cos \alpha \end{pmatrix} |1\rangle}{\sqrt{2}} =$$

$$\frac{\cos \alpha |00\rangle + \sin \alpha |10\rangle + \sin \alpha |01\rangle - \cos \alpha |11\rangle}{\sqrt{2}} = \cos \alpha |\phi_-\rangle + \sin \alpha |\psi_+\rangle$$



### סעיף 3.3:

תחילה נחשב את תוצאת הפעלת  $R_\alpha$  על המצב  $|\psi_+\rangle$ :

$$R_\alpha \otimes I |\psi_+\rangle = \frac{(R_\alpha |0\rangle)|1\rangle - (R_\alpha |1\rangle)|0\rangle}{\sqrt{2}} = \frac{\begin{pmatrix} \cos \alpha \\ \sin \alpha \end{pmatrix} |1\rangle - \begin{pmatrix} -\sin \alpha \\ \cos \alpha \end{pmatrix} |0\rangle}{\sqrt{2}} =$$

$$\frac{\cos \alpha |01\rangle + \sin \alpha |11\rangle - \sin \alpha |00\rangle + \cos \alpha |10\rangle}{\sqrt{2}} = \cos(-\alpha) |\psi_+\rangle + \sin(-\alpha) |\phi_-\rangle$$

כעת, נגרום לאליס להפעיל את  $R_\alpha$  ולבוב להפעיל את  $R_{-\beta}$  ונראה שזה

יגרום למצב המבוקש.

$$(R_\alpha R_{-\beta}) \otimes I |\phi_-\rangle \stackrel{3.2}{=} R_\alpha (\cos(-\beta) |\phi_-\rangle + \sin(-\beta) |\psi_+\rangle) =$$

$$\cos(-\beta) (\cos \alpha |\phi_-\rangle + \sin \alpha |\psi_+\rangle) + \sin(-\beta) (\cos(-\alpha) |\psi_+\rangle + \sin(-\alpha) |\phi_-\rangle) =$$

$$(\cos \alpha \cos \beta + \sin \alpha \sin \beta) |\phi_-\rangle + (\sin \alpha \cos \beta - \cos \alpha \sin \beta) |\psi_+\rangle \stackrel{\text{trig sum identities}}{=} \cos(\alpha - \beta) |\phi_-\rangle + \sin(\alpha - \beta) |\psi_+\rangle$$

$$P(\text{same res}) = P(\text{both get 0}) + P(\text{both get 1}) = P(|00\rangle) + P(|11\rangle) =$$

$$\frac{\cos^2(\alpha - \beta)}{2} + \frac{\cos^2(\alpha - \beta)}{2} = \cos^2(\alpha - \beta)$$

### סעיף 3.4:

נסמן את ערכי  $\alpha$  של אליס בהינתן הקלטים 0,1 ב-  $\alpha_0, \alpha_1$  בהתאמה

וכמו כן את של בוב ב  $\beta_0, \beta_1$ .

לכן ההסת' להצלחה בהנתן הקלט 00 היא ההסת' שהם יבחרו את אותו ביט, שכפי שראינו נתונה על ידי  $\cos^2(\alpha_0 - \beta_0)$ . כמו כן, במקרים שהקלט הוא 01 או 10 הפלט המצופה זהה ולכן ההסת' נתונות על ידי

$$\cos^2(\alpha_1 - \beta_0) \text{ ו- } \cos^2(\alpha_0 - \beta_1) \text{ בהתאמה.}$$

עבור הקלט 11 ההסת' להצלחה היא ההסת' שהם לא יבחרו אותו ביט,

$$\text{כלומר } 1 - \cos^2(\alpha_1 - \beta_1) = \sin^2(\alpha_1 - \beta_1)$$

מאחר וההתפלגות אחידה על פני הקלטים, ההסתברות הכוללת

$$\text{להצלחה תהיה } \frac{\cos^2(\alpha_0 - \beta_0) + \cos^2(\alpha_0 - \beta_1) + \cos^2(\alpha_1 - \beta_0) + \sin^2(\alpha_1 - \beta_1)}{4}$$

$$\text{בחירת הערכים } \alpha_0 = 0, \alpha_1 = \frac{3}{4}\pi, \beta_0 = \frac{-1}{8}\pi, \beta_1 = \frac{1}{8}\pi$$

מביאה את ההסת' למקסימום שהינו בקירוב 0.853.

הפתרון התקבל נומרית אחרי צמצום הבעיה לכך ש  $\alpha_0 \neq \alpha_1$

וכן ש-  $\beta_0 = -\beta_1$ , (כי אחרת ההסת' המקסימלית שניתן לקבל היא  $\frac{3}{4}$ )

לאחר מכן השתמשנו בפתרון נומרי ומחלוקתו ב  $\pi$  קיבלנו את המקדמים.

## שאלה 4:

### סעיף 4.1.1:

$$\alpha|000\rangle + \beta|100\rangle \xrightarrow{\text{CNOT}_{12}} \alpha|000\rangle + \beta|110\rangle \xrightarrow{\text{CNOT}_{13}} \alpha|000\rangle + \beta|111\rangle$$

### סעיף 4.1.2:

$$I|\psi'\rangle = \alpha|000\rangle + \beta|111\rangle \xrightarrow{\text{CNOT}_{12}} \alpha|000\rangle + \beta|101\rangle \xrightarrow{\text{CNOT}_{13}} \alpha|000\rangle + \beta|100\rangle = |\psi\rangle|00\rangle$$

$$X_1|\psi'\rangle = \alpha|100\rangle + \beta|011\rangle \xrightarrow{\text{CNOT}_{12}} \alpha|110\rangle + \beta|011\rangle \xrightarrow{\text{CNOT}_{13}} \alpha|111\rangle + \beta|011\rangle \rightarrow \alpha|011\rangle + \beta|111\rangle = |\psi\rangle|11\rangle$$

$$X_2|\psi'\rangle = \alpha|010\rangle + \beta|101\rangle \xrightarrow{\text{CNOT}_{12}} \alpha|010\rangle + \beta|111\rangle \xrightarrow{\text{CNOT}_{13}} \alpha|010\rangle + \beta|110\rangle \rightarrow \alpha|010\rangle + \beta|110\rangle = |\psi\rangle|10\rangle$$

$$X_3|\psi'\rangle = \alpha|001\rangle + \beta|110\rangle \xrightarrow{\text{CNOT}_{12}} \alpha|001\rangle + \beta|100\rangle \xrightarrow{\text{CNOT}_{13}} \alpha|001\rangle + \beta|101\rangle \rightarrow \alpha|001\rangle + \beta|101\rangle = |\psi\rangle|01\rangle$$

### סעיף 4.2.1:

$$\alpha|000\rangle + \beta|100\rangle \rightarrow \text{CNOT} \rightarrow \alpha|000\rangle + \beta|111\rangle \rightarrow \text{H} \rightarrow \alpha|+++ \rangle + \beta|--- \rangle$$

### סעיף 4.2.2:

$$I|\psi''\rangle = \alpha|+++ \rangle + \beta|--- \rangle \rightarrow \text{H} \rightarrow \alpha|000\rangle + \beta|111\rangle \rightarrow \text{CNOT} \rightarrow \alpha|000\rangle + \beta|100\rangle$$

$$\rightarrow \text{CNOT} \rightarrow \alpha|000\rangle + \beta|100\rangle = |\psi\rangle|00\rangle$$

$$Z_1|\psi''\rangle = \alpha| - + + \rangle + \beta| + - - \rangle \rightarrow \text{H} \rightarrow \alpha|100\rangle + \beta|011\rangle \rightarrow \text{CNOT} \rightarrow \alpha|110\rangle + \beta|011\rangle$$

$$\rightarrow \text{CNOT} \rightarrow \alpha|111\rangle + \beta|011\rangle \rightarrow \text{CNOT} \rightarrow \alpha|011\rangle + \beta|111\rangle = |\psi\rangle|11\rangle$$

$$Z_2|\psi''\rangle = \alpha| + - + \rangle + \beta| - + - \rangle \rightarrow \text{H} \rightarrow \alpha|010\rangle + \beta|101\rangle \rightarrow \text{CNOT} \rightarrow \alpha|010\rangle + \beta|111\rangle$$

$$\rightarrow \text{CNOT} \rightarrow \alpha|010\rangle + \beta|110\rangle \rightarrow \text{CNOT} \rightarrow \alpha|010\rangle + \beta|110\rangle = |\psi\rangle|10\rangle$$

$$Z_3|\psi''\rangle = \alpha| + + - \rangle + \beta| - - + \rangle \rightarrow \text{H} \rightarrow \alpha|001\rangle + \beta|110\rangle \rightarrow \text{CNOT} \rightarrow \alpha|001\rangle + \beta|100\rangle$$

$$\rightarrow \text{CNOT} \rightarrow \alpha|001\rangle + \beta|101\rangle \rightarrow \text{CNOT} \rightarrow \alpha|001\rangle + \beta|101\rangle = |\psi\rangle|01\rangle$$

### סעיף 4.3.1: תחילה נסמן חזקה $n$ של מצב קוונטי כמכפלה טמורית

של המצב עם עצמו n פעמים.

$$\begin{aligned}
 & \alpha|0^9\rangle + \beta|10^8\rangle \rightarrow \text{---} \rightarrow \alpha|000\rangle^3 + \beta|100\rangle^3 \rightarrow \text{---} \rightarrow \alpha|+00\rangle^3 + \beta|-00\rangle^3 \rightarrow \text{---} \\
 & \rightarrow \alpha \left( \frac{|000\rangle + |110\rangle}{\sqrt{2}} \right)^3 + \beta \left( \frac{|000\rangle - |110\rangle}{\sqrt{2}} \right)^3 \rightarrow \text{---} \\
 & \rightarrow \alpha \left( \frac{|000\rangle + |111\rangle}{\sqrt{2}} \right)^3 + \beta \left( \frac{|000\rangle - |111\rangle}{\sqrt{2}} \right)^3
 \end{aligned}$$

זהו בדיוק הפלט המצופה תחת הסימון המקוצר.

### סעיף 4.3.2:

$$\begin{aligned}
I|\psi'''\rangle &= \alpha \left( \frac{|000\rangle + |111\rangle}{\sqrt{2}} \right)^3 + \beta \left( \frac{|000\rangle - |111\rangle}{\sqrt{2}} \right)^3 \rightarrow \alpha \left( \frac{|000\rangle + |100\rangle}{\sqrt{2}} \right)^3 + \beta \left( \frac{|000\rangle - |100\rangle}{\sqrt{2}} \right)^3 \rightarrow \\
&\rightarrow \alpha \left( \frac{|+00\rangle + |-00\rangle}{\sqrt{2}} \right)^3 + \beta \left( \frac{|+00\rangle - |-00\rangle}{\sqrt{2}} \right)^3 = \alpha \left( \frac{|000\rangle + |100\rangle + |000\rangle - |100\rangle}{2} \right)^3 + \\
&\rightarrow \alpha \left( \frac{|000\rangle + |100\rangle - |000\rangle + |100\rangle}{2} \right)^3 \rightarrow \alpha|000\rangle^3 + \beta|100\rangle^3 \rightarrow \alpha|000\rangle^3 + \beta|10^8\rangle \rightarrow \alpha|000\rangle^3 + \beta|10^8\rangle = |\psi\rangle|0^8\rangle
\end{aligned}$$





## 5. A

BHM96 quantum key distribution (QKD) protocol is correct:

At the beginning of the protocol, Alice and Bob both randomly choose one of the four states  $\{|0i\rangle, |1i\rangle, |+i\rangle, |-i\rangle\}$  and send it to the center. They secretly keep the bit they sent in the same way as described in the protocol: Alice keeps bit 0 if she sent the state  $|0i\rangle$  or  $|+i\rangle$ , and keeps bit 1 otherwise; Bob does the same.

The center measures the two qubits it received in the Bell basis, which is defined as the following four states:


$$|\varphi^{++}\rangle = (|0i\rangle \otimes |0i\rangle + |1i\rangle \otimes |1i\rangle) / \sqrt{2}$$

$$|\varphi^{--}\rangle = (|0i\rangle \otimes |0i\rangle - |1i\rangle \otimes |1i\rangle) / \sqrt{2}$$

$$|\varphi^{0+}\rangle = (|0i\rangle \otimes |1i\rangle + |1i\rangle \otimes |0i\rangle) / \sqrt{2}$$

$$|\varphi^{1+}\rangle = (|0i\rangle \otimes |1i\rangle - |1i\rangle \otimes |0i\rangle) / \sqrt{2}$$


The center reports the measurement result to Alice and Bob.

In step 4, Alice and Bob compare the bases they used (the calculation base or Damard base) and the measurement result of the center. If the bases are equal and the result of the measurement of the center, as reported to both Alice and Bob, is  $|\varphi^{++}\rangle$  or  $|\varphi^{--}\rangle$ , Alice and Bob keep the bit (Bob reverses his bit, i.e.  changes 0 to 1 and 1 to 0; Alice does nothing). Otherwise, Alice and Bob discard the bit.

If Alice and Bob both used the same base and the center's measurement result is  $|\varphi^{++}\rangle$  or  $|\varphi^{--}\rangle$ , then the bit they kept is the same.

This is because the state they sent to the center is the same, and the center's measurement result is the same.

For example, if both Alice and Bob used the calculation base and the center's measurement result is  $|\varphi^{++}\rangle$ , then both Alice and Bob will keep the same bit.

If the center used a different  base, or the measurement result was different, then Alice and Bob both discard the bit

. This means that the center has no information about the bit values, even if it listens to all the classical communication exchanged between Alice and Bob in step 4.

Therefore, the BHM96 QKD protocol is correct because it ensures that Alice and Bob share the same key, and the center has no information about the key.

## 5.B

Analyze what happens if the center tries to attack Alice and Bob: instead of measuring in the Bell base, the center measures in the base  $\{|11i, |10i, |01i, |00i\}$  to find out the bit values. Will Alice and Bob notice this attack, and how? What will be the percentage of errors will Alice and Bob accept?

If the center tries to attack Alice and Bob by measuring in the  $\{|11i, |10i, |01i, |00i\}$  basis instead of the Bell basis, Alice and Bob will notice this attack because their bases and the measurement result reported by the center will not match. This is because the  $\{|11i, |10i, |01i, |00i\}$  basis is not compatible with the calculation or Damard bases that Alice and Bob are using. When Alice and Bob compare the bases they used and the measurement result of the center, they will find that the bases do not match, and they will discard the bit.

This means that the percentage of errors that Alice and Bob accept will be 100%, as they will discard all the bits.



Here's an example:

At the beginning of the protocol, Alice and Bob both randomly choose one of the four states  $\{|0i, |1i, |+i, |-i\}$  and send it to the center. They secretly keep the bit they sent in the same way as described in the

protocol:

Alice keeps bit 0 if she sent the state  $|0i$  or  $|+i$ , and keeps bit 1 otherwise; Bob does the same.

In this case, let's say Alice sends the state  $|0i$ , and Bob sends the state  $|1i$ . The center, instead of measuring in the Bell basis, measures in the  $\{|11i, |10i, |01i, |00i\}$  basis and reports the measurement result to Alice and Bob.

The  $\{|11i, |10i, |01i, |00i\}$  basis is defined as follows:

$$|\psi_0\rangle = |11i \quad |\psi_1\rangle = |10i \quad |\psi_2\rangle = |01i \quad |\psi_3\rangle = |00i$$

In step 4, Alice and Bob compare the bases they used (the calculation base or Damard base) and the measurement result of the center. If the bases are equal and the result of the measurement of the center, as reported to both Alice and Bob, is  $|\psi_+\rangle$  or  $|\psi_-\rangle$ , Alice and Bob keep the bit (Bob reverses his bit, i.e. changes 0 to 1 and 1 to 0; Alice does nothing). Otherwise, Alice and Bob discard the bit.

In this case, Alice and Bob both used the calculation base, but the center used the  $\{|11i, |10i, |01i, |00i\}$  basis.

Therefore, the bases do not match, and Alice and Bob will discard the bit. The percentage of errors that Alice and Bob accept in this case will be 100%.

# 5.C



Analyze what happens if the center tries to attack Alice and Bob: instead of measuring in the Bell base, the center measures in the base  $\{|11i, |10i, |01i, |00i\}$  to find out the bit values. Will Alice and Bob notice this attack, and how? What will be the percentage of errors will Alice and Bob accept?

If the center tries to attack Alice and Bob by measuring in the  $\{|11i, |10i, |01i, |00i\}$  basis instead of the Bell basis, Alice and Bob will notice this attack because their bases and the measurement result reported by the center will not match. This is because the  $\{|11i, |10i, |01i, |00i\}$  basis is not compatible with the calculation or Damard bases that Alice and Bob are using. When Alice and Bob compare the bases they used and the measurement result of the center, they will find that the bases do not match, and they will discard the bit.

This means that the percentage of errors that Alice and Bob accept will be 100%, as they will discard all the bits.

Here's an example:

At the beginning of the protocol, Alice and Bob both randomly choose one of the four states  $\{|0i, |1i, |+i, |-i\}$  and send it to the center. They secretly keep the bit they sent in the same way as described in the

protocol:

Alice keeps bit 0 if she sent the state  $|0i$  or  $|+i$ , and keeps bit 1 otherwise; Bob does the same.

In this case, let's say Alice sends the state  $|0i$ , and Bob sends the state  $|1i$ . The center, instead of measuring in the Bell basis, measures in the  $\{|11i, |10i, |01i, |00i\}$  basis and reports the measurement result to Alice and Bob.

The  $\{|11i, |10i, |01i, |00i\}$  basis is defined as follows:

$$|\psi_0\rangle = |11i \quad |\psi_1\rangle = |10i \quad |\psi_2\rangle = |01i \quad |\psi_3\rangle = |00i$$

In step 4, Alice and Bob compare the bases they used (the calculation base or Damard base) and the measurement result of the center. If the bases are equal and the result of the measurement of the center, as reported to both Alice and Bob, is  $|\psi_+\rangle$  or  $|\psi_-\rangle$ , Alice and Bob keep the bit (Bob reverses his bit, i.e. changes 0 to 1 and 1 to 0; Alice does nothing). Otherwise, Alice and Bob discard the bit.

In this case, Alice and Bob both used the calculation base, but the center used the  $\{|11i, |10i, |01i, |00i\}$  basis.

Therefore, the bases do not match, and Alice and Bob will discard the bit. The percentage of errors that Alice and Bob accept in this case will be 100%.

## 5.C



if the center tries to attack Alice and Bob by measuring in the  $\{|i, |--i, |-+i, |+ -i\}$  basis instead of the Bell basis:

At the beginning of the protocol, Alice and Bob both randomly choose one of the four states  $\{|0i, |1i, |+i, |-i\}$  and send it to the center. They secretly keep the bit they sent in the same way as described in the protocol: Alice keeps bit 0 if she sent the state  $|0i$  or  $|+i$ , and keeps bit 1 otherwise; Bob does the same.

In this case, let's say Alice sends the state  $|0i$ , and Bob sends the state  $|1i$ . The center, instead of measuring in the Bell basis, measures in the  $\{|i, |--i, |-+i, |+ -i\}$  basis and reports the measurement result to Alice and Bob.

The  $\{|i, |--i, |-+i, |+ -i\}$  basis is defined as follows:

$$|\varphi_0\rangle = |i\rangle \quad |\varphi_1\rangle = |--i\rangle \quad |\varphi_2\rangle = |-+i\rangle \quad |\varphi_3\rangle = |+ -i\rangle$$

In step 4, Alice and Bob compare the bases they used (the calculation base or Damard base) and the measurement result of the center. If the bases are equal and the result of the measurement of the center, as reported to both Alice and Bob, is  $|\varphi_+\rangle$  or  $|\varphi_-\rangle$ , Alice and Bob keep the bit (Bob reverses his bit, i.e. changes 0 to 1 and 1 to 0; Alice does nothing). Otherwise, Alice and Bob discard the bit.

In this case, Alice and Bob both used the calculation base, but the center used the  $\{|i, |--i, |-+i, |+ -i\}$  basis. Therefore, the bases do not match, and Alice and Bob will discard the bit. The percentage of errors that Alice and Bob accept in this case will be 100%.