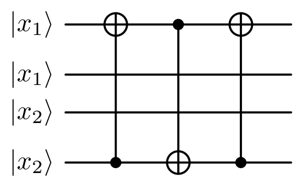
Problem 10. Quantum encryption

Dung Le Quoc

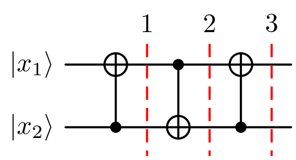
December 27, 2023

1 Analyze circuit before Hadamard gates

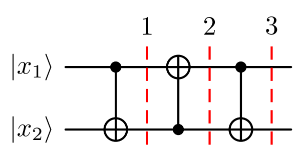
We analyze the above half of circuit ($|x_1\rangle$ and $|x_2\rangle$). The below half is similar.



Let's analyze first and fourth lines.



On the first red verticle line, the CNOT gate gives us $|x_1 \oplus x_2\rangle$ and $|x_2\rangle$.
On the second red verticle line, the CNOT gate give us $|x_1 \oplus x_2\rangle$ and $|x_2 \oplus x_1 \oplus x_2\rangle = |x_1\rangle$.
On the third red verticle line, the CNOT gate give us $|x_1 \oplus x_2 \oplus x_1\rangle = |x_2\rangle$ and $|x_1\rangle$.
Similarly, for second and third line.



On the first red verticle line, the CNOT gate gives us $|x_1\rangle$ and $|x_2 \oplus x_1\rangle$.
On the second red verticle line, the CNOT gate gives us $|x_1 \oplus x_2 \oplus x_1\rangle = |x_2\rangle$ and $|x_2 \oplus x_1\rangle$.
On the third red verticle line, the CNOT gate gives us $|x_2\rangle$ and $|x_2 \oplus x_1 \oplus x_2\rangle = |x_1\rangle$.
So, in fact, this circuit give us figure 1.

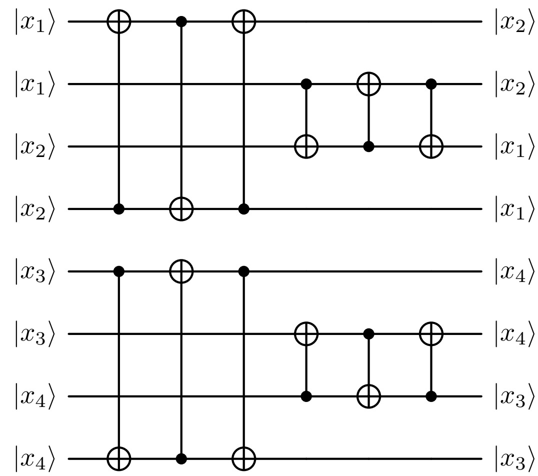


Figure 1: Circuit before Hadamard gates

2 Analyze circuit after Hadamard gates

Suppose that $H^{k_i}(|x_j\rangle) = |z_j\rangle$. After the H^{k_i} gate, we have figure 2.

We need to notice that, if $k_i = 0$, then $|x_j\rangle$ becomes $|x_j\rangle$ (Hadamard gate is not considered). And if $k_i = 1$, then $|x_i\rangle$ becomes $\dfrac{|0\rangle + (-1)^{x_j}|1\rangle}{\sqrt{2}} = |z_j\rangle$. We can see that coefficient before $|0\rangle$ is not negative for all cases of x_j and k_i (0, 1 or $\dfrac{1}{\sqrt{2}}$).

After that, qubits $|z_i\rangle$ go through CNOT gates (figure 3).

At each verticle red line, one qubit will control one other qubit by CNOT gate. Actually, CNOT gate is a matrix that has property: on each row and on each column there is only one element and it equals to 1.

For example, with two qubits with product $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$. We know that CNOT gate actually is the matrix multiplication

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{11} \\ \alpha_{10} \end{pmatrix} \tag{1}$$

It means that $\text{CNOT}|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{11}|10\rangle + \alpha_{10}|11\rangle$.

Now we consider three qubits. Their product will have form

$$|\psi\rangle = \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle + \alpha_{100}|100\rangle + \alpha_{101}|101\rangle + \alpha_{110}|110\rangle + \alpha_{111}|111\rangle$$

If the first qubit controls the third qubit by CNOT gate, this is equivalent with exchanging coefficient of $|1x0\rangle$ and $|1x1\rangle$, where $x \in \{0, 1\}$.

As the result, we receive the product after the first qubit had controlled the third qubit as following

$$|\psi'\rangle = \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle + \alpha_{101}|100\rangle + \alpha_{100}|101\rangle + \alpha_{111}|110\rangle + \alpha_{110}|111\rangle$$

$$|x_2\rangle \;—\; \boxed{H^{k_1}} \;—\; |z_2\rangle$$

$$|x_2\rangle \;—\; \boxed{H^{k_1}} \;—\; |z_2\rangle$$

$$|x_1\rangle \;—\; \boxed{H^{k_2}} \;—\; |z_1\rangle$$

$$|x_1\rangle \;—\; \boxed{H^{k_2}} \;—\; |z_1\rangle$$

$$|x_4\rangle \;—\; \boxed{H^{k_3}} \;—\; |z_4\rangle$$

$$|x_4\rangle \;—\; \boxed{H^{k_3}} \;—\; |z_4\rangle$$

$$|x_3\rangle \;—\; \boxed{H^{k_4}} \;—\; |z_3\rangle$$

$$|x_3\rangle \;—\; \boxed{H^{k_4}} \;—\; |z_3\rangle$$

Figure 2: Key K acts on qubits

Here, the matrix for multiplication is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha_{000} \\ \alpha_{001} \\ \alpha_{010} \\ \alpha_{011} \\ \alpha_{100} \\ \alpha_{101} \\ \alpha_{110} \\ \alpha_{111} \end{pmatrix} = \begin{pmatrix} \alpha_{000} \\ \alpha_{001} \\ \alpha_{010} \\ \alpha_{011} \\ \alpha_{101} \\ \alpha_{100} \\ \alpha_{111} \\ \alpha_{110} \end{pmatrix} \tag{2}$$

In other word, we can notice that the set of coefficients is unchanged. The coefficients only move from one amplitude to the other.

So, if I let $|z_2\rangle = a|0\rangle + b|1\rangle$, $|z_1\rangle = c|0\rangle + d|1\rangle$, $|z_4\rangle = e|0\rangle + f|1\rangle$, and $|z_3\rangle = g|0\rangle + h|1\rangle$, then the state right after Hadamard gates is

$$|z_2\rangle \otimes |z_2\rangle \otimes |z_1\rangle \otimes |z_1\rangle \otimes |z_4\rangle \otimes |z_4\rangle \otimes |z_3\rangle \otimes |z_3\rangle \tag{3}$$

Notice that $|z_2\rangle \otimes |z_2\rangle = (a|0\rangle + b|1\rangle) \otimes (a|0\rangle + b|1\rangle) = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle$. We see that in this product there are three different coefficients, and we need all three coefficients (a^2, ab, b^2) to determine a and b, in other word - determine $|z_2\rangle$. This is because $b^2 = (-b)^2$, we need ab in order to make sure that the product of square root is not $-ab$, and we has already known that a is not negative (more precisely, 0, 1, or $\frac{1}{\sqrt{2}}$).

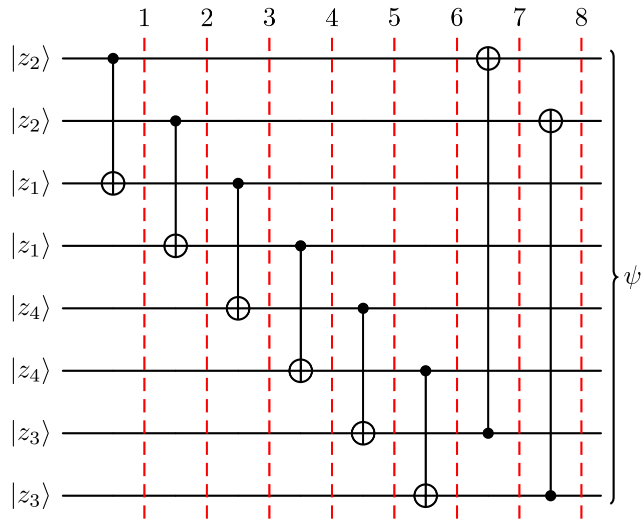


Figure 3: CNOT gates after Hadamard gates

We have 4 product $|z_i\rangle \otimes |z_i\rangle$, each need 3 (instead of 4) coefficients to recover qubit $|z_i\rangle$. So we only need $3^4 = 81$ amplitudes to get the key, instead of 256.

So the answer is 81.