



Problem 12. «A quantum cipher»

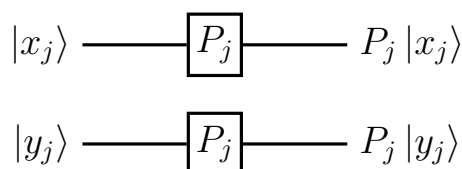
Alice invented the following quantum symmetric cipher. The plaintext is encoded into the sequence of n pairs of qubit states $|x_1\rangle|y_1\rangle, |x_2\rangle|y_2\rangle, \dots, |x_n\rangle|y_n\rangle$, where $|x_j\rangle, |y_j\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, $j = 1, 2, \dots, n$. Here $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ are Hadamard states. The secret key k is a random vector from the set $\{0, 1, 2, 3\}^n$. On iteration j , depending on the value k_j , some Pauli gate $P_j \in \{I, X, Y, Z\}$ is chosen:

k_j	P_j
0	I
1	X
2	Y
3	Z

Note that any quantum gate is a unitary operator that acts on the space of the states of the corresponding quantum system. The used Pauli gates together with identical one are

Identity gate I	$ x\rangle \xrightarrow{I} x\rangle$	acts on a single qubit in the state $ x\rangle$
Pauli X gate	$ x\rangle \xrightarrow{X} x \oplus 1\rangle$	acts on a single qubit in the state $ x\rangle$
Pauli Y gate	$ x\rangle \xrightarrow{Y} i(-1)^x 1-x\rangle$	acts on a single qubit in the state $ x\rangle$
Pauli Z gate	$ x\rangle \xrightarrow{Z} (-1)^x x\rangle$	acts on a single qubit in the state $ x\rangle$

Here $x \in \{0, 1\}$. The chosen gate acts on every qubit from the corresponding pair: $|x_j\rangle \otimes |y_j\rangle \rightarrow (P_j |x_j\rangle) \otimes (P_j |y_j\rangle)$. The state $(P_j |x_j\rangle) \otimes (P_j |y_j\rangle)$ is the result of the encryption of j -th pair $|x_j\rangle|y_j\rangle$, this process can be described by the quantum circuit Q :



Assume that the same key $(k_1, k_2, \dots, k_n)$ can be used for more than one encryption. Describe in details possible vulnerabilities of the cipher that Eve could use in order to obtain information about the key or the plaintext qubit states.

Remark. Let us briefly formulate the key points of quantum circuits. A qubit is a two-level quantum mechanical system whose state $|\psi\rangle$ is the superposition of basis orthonormal quantum states $|0\rangle$ and $|1\rangle$. The superposition is written as $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$, where α_0 and α_1 are complex numbers, called

amplitudes, that possess $|\alpha_0|^2 + |\alpha_1|^2 = 1$. The amplitudes α_0 and α_1 have the following physical meaning: after the measurement of a qubit which has the state $|\psi\rangle$ in a basis $\{|0\rangle, |1\rangle\}$, it will be found in the state $|0\rangle$ with probability $|\alpha_0|^2$ and in the state $|1\rangle$ with probability $|\alpha_1|^2$. One can also write $|\psi\rangle = \alpha'_0|+\rangle + \alpha'_1|-\rangle$, where amplitudes α'_0, α'_1 possess the same norm condition and characterize the probabilities of observing the system in the states $|+\rangle$ and $|-\rangle$.

In order to operate with multi-qubit systems, we consider the bilinear operation $\otimes : |x\rangle, |y\rangle \rightarrow |x\rangle \otimes |y\rangle$ on $x, y \in \{0, 1\}$ which is defined on pairs $|x\rangle, |y\rangle$, and by bilinearity is expanded on the space of all linear combinations of $|0\rangle$ and $|1\rangle$. When we have two unentangled (separable) qubits in states $|\psi\rangle$ and $|\varphi\rangle$ correspondingly, the state of the whole system of these two qubits is $|\psi\rangle \otimes |\varphi\rangle$. In general, for two qubits we have $|\psi\rangle = \alpha_{00}|0\rangle \otimes |0\rangle + \alpha_{01}|0\rangle \otimes |1\rangle + \alpha_{10}|1\rangle \otimes |0\rangle + \alpha_{11}|1\rangle \otimes |1\rangle$. The physical meaning of complex numbers α_{ij} is the same as for one qubit, so we have the essential restriction $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. For brevity one can write $|a\rangle \otimes |b\rangle \equiv |ab\rangle$.

In fact the state can also be written in other orthonormal basis, for example one can consider four Bell states

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),$$

or

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle),$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|++\rangle - |--\rangle),$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|+-\rangle + |-+\rangle),$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle).$$

Then for the state of the system of two qubits we have $|\psi\rangle = \alpha_{\Phi^+}|\Phi^+\rangle + \alpha_{\Phi^-}|\Phi^-\rangle + \alpha_{\Psi^+}|\Psi^+\rangle + \alpha_{\Psi^-}|\Psi^-\rangle$.

The physical meaning of amplitudes $\alpha_{\Phi^+}, \alpha_{\Phi^-}, \alpha_{\Psi^+}, \alpha_{\Psi^-}$ is the same as before.