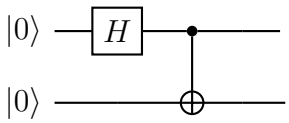
Problem 7. «Try your quantum skills!»

In oder to use the quantum cryptanalysis techniques one should be able to work with quantum bits. Daniel knows little about quantum circuits but wants to try his hand at a new field! **A quantum circuit** is a scheme where we operate with some set of qubits. The operations include one- or multi-qubit transformations provided by so called **quantum gates**. They are characterized by unitary operators that act on the space of qubits. An example of a quantum circuit is the following:



$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

It transforms the state $|00\rangle$ to the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The upper wire corresponds to the action on the first qubit while the lower corresponds to the second one. Here, we have the following transformations: $|00\rangle \xrightarrow{H,\text{ 1st qubit}} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \xrightarrow{CNOT,\text{ both qubits}} \frac{1}{\sqrt{2}} CNOT\,|00\rangle + \frac{1}{\sqrt{2}} CNOT\,|10\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Q1 Given the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, design a circuit that transforms $|\psi\rangle$ to the state $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

Q2 Design the circuit that distinguishes between the entangled states $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. Distinguishing means that after the measurement of the final state we can exactly say what the state from these three was given. Use the list of gates presented below.

Remark. A qubit is a two-level quantum mechanical system whose state $|\psi\rangle$ is the superposition of basis 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 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 $|\psi\rangle$, it will be found in the state $|0\rangle$ with probability $|\alpha_0|^2$ and in the state $|1\rangle$ with probability $|\alpha_1|^2$. In order to operate with multi-qubit systems, we consider the bilinear operation $\otimes : |x\rangle, |y\rangle \to |x\rangle \otimes |y\rangle$ 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 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 $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. We use more brief notation $|a\rangle \otimes |b\rangle \equiv |ab\rangle$.

Pauli-X gate	$\|x\rangle$ — X — $\|x \oplus 1\rangle$	acts on a single qubit in the state $\|x\rangle$, $x \in \{0, 1\}$
Pauli-Z gate	$\|x\rangle$ — Z — $(-1)^x \|x\rangle$	acts on a single qubit in the state $\|x\rangle$, $x \in \{0, 1\}$
Hadamard gate	$\|x\rangle$ — H — $\frac{\|0\rangle + (-1)^x \|1\rangle}{\sqrt{2}}$	acts on a single qubit in the state $\|x\rangle$, $x \in \{0, 1\}$
controlled NOT (CNOT) gate	$\|x\rangle$ — $\|x\rangle$; $\|y\rangle$ — $\|y \oplus x\rangle$	acts on a pair of qubits in the states $\|x\rangle, \|y\rangle$, $x, y \in \{0, 1\}$
SWAP gate	$\|x\rangle$ — $\|y\rangle$; $\|y\rangle$ — $\|x\rangle$	acts on a pair of qubits in the states $\|x\rangle, \|y\rangle$, $x, y \in \{0, 1\}$