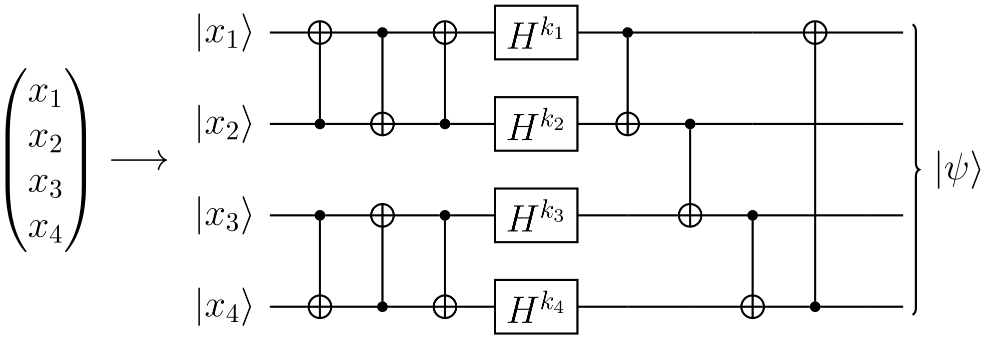
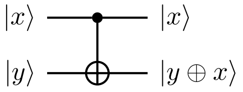
Problem 10. «Quantum encryption»

Bob works in a field of quantum mechanics and he has some ideas how it can be applied for the encryption of secret messages. He developed a toy cipher that encrypts 4-bit words by using 4-bit secret key $\left(k_1, k_2, k_3, k_4\right)$ and the following quantum circuit:



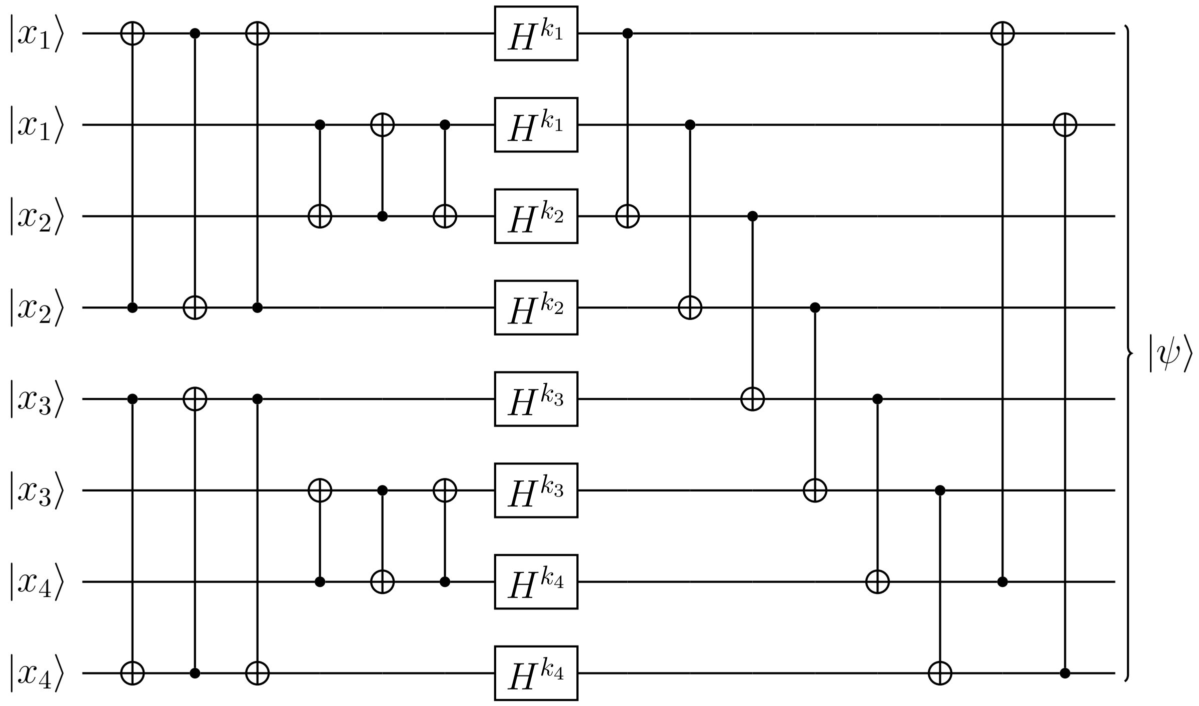
This cipher operates with 4-bit plaintext $\left(x_1, x_2, x_3, x_4\right)$ that is initially encoded to the corresponding 4-qubit «plainstate» $|x_1, x_2, x_3, x_4\rangle$. This quantum state is an input of the circuit that consists of several single-qubit gates. Note that any quantum gate is a unitary operator that acts on the space of the states of the corresponding quantum system. The used gates are

Hadamard gate	$|x\rangle$ — $\boxed{H}$ — $\frac{|0\rangle+(-1)^x|1\rangle}{\sqrt{2}}$	acts on a single qubit in the state $|x\rangle$, $x \in \{0,1\}$
CNOT gate	 $|x\rangle$ $|x\rangle$ $|y\rangle$ $|y \oplus x\rangle$	acts on a pair of qubits in the states $|x\rangle$, $|y\rangle$, $x, y \in \{0,1\}$

The notation H^b, where $b \in \{0,1\}$, means that if $b = 0$, the identity gate I is applied instead of H, while for $b = 1$ the gate H is considered.

The result of the encryption is the «cipherstate» $|\psi\rangle$ that is further transmitted via the quantum channel. The decryption procedure takes the state $|\psi\rangle$ and applies the inverse circuit.

Bob was advised to increase the number of qubits in order to reduce the effect of possible errors in quantum computation and quantum channel, so he decided to modify the circuit and make copies of qubits of the plainstate. The resulting circuit is the following:



Alice looked at the cipher and claimed that she would be able to reveal the secret key (k_1, k_2, k_3, k_4) if she knew some number N of certain amplitudes of the state $|\psi\rangle$. The state $|\psi\rangle$ is characterized by 256 amplitudes, so essentially we have $N \leqslant 256$.

Could you check the assumption of Alice and find the least possible value of N if the claim is correct?

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 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 $|\psi\rangle$, 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 $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. By induction, this process is expanded on the case of three qubits and more. Thus, the general form of the state of n qubits is

$$|\psi\rangle = \sum_{x \in \mathbb{F}_2^n} \alpha_x |x\rangle,$$

where amplitudes $\alpha_{00\ldots0}, \alpha_{00\ldots01}, \ldots, \alpha_{11\ldots1}$ have the same physical meaning as discussed before. Here we use more brief notation $|x_1\rangle \otimes |x_2\rangle \otimes \ldots \otimes |x_n\rangle \equiv |x_1, x_2, \ldots, x_n\rangle \equiv |x_1 x_2 \ldots x_n\rangle$.