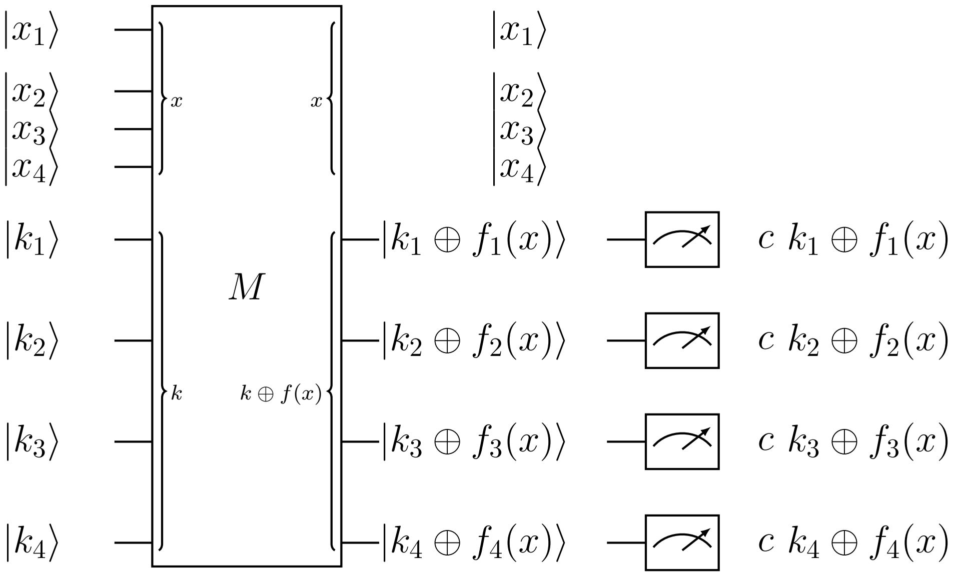
Problem 8. «Unknown function»

Bob works in a field of quantum mechanics, he invented a quantum machine M that encrypts 4-bit words by using 4-bit secret key $k = (k_1, k_2, k_3, k_4)$ according to the following quantum circuit:



This machine operates with 4-bit plaintext $x = (x_1, x_2, x_3, x_4)$ that is initially encoded to the corresponding 4-qubit «plainstate» $|x_1, x_2, x_3, x_4\rangle$ that is both with the «keystate» $|k_1, k_2, k_3, k_4\rangle$ is operated as

$$|x\rangle\,|k\rangle \xrightarrow{M} |x\rangle\,|k \oplus f(x)\rangle\,,$$

where $f(x) = (f_1(x), f_2(x), f_3(x), f_4(x))$ is an invertible vectorial Boolean function in 4 variables. The «cipherstate» $|k_1 \oplus f_1(x), k_2 \oplus f_2(x), k_3 \oplus f_3(x), k_4 \oplus f_4(x)\rangle$ is further measured and the ciphertext is obtained.

The problem is could Alice find the secret key k if the function f is unknown to her? Assume she has oracle access to the quantum machine with the fixed key k and she provided additional information $f(0,0,0,0) \oplus f(1,1,1,1) \oplus f(1,0,0,0) = c \in \mathbb{F}_2^4$ with known c.

Remark. Recall some 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 satisfy $|\alpha_0|^2 + |\alpha_1|^2 = 1$. The amplitudes α_0 and α_1 have the following physical meaning: after the measurement of a qubit with 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 $|\alpha_1|^2$. After the computation, the state of the qubit is measered and the result is observed.