NSUCRYPTO2024

Problem 10: Unknown function

October 21, 2024

Solution

Send $x_1 = (0,0,0,0)$ and $x_2 = (1,1,1,1)$ to the oracle, we receive $c_1 = k \oplus f(x_1)$ and $c_2 = k \oplus f(x_2)$.

Observe that:

$$\begin{aligned} c_1 \oplus c_2 &= (f_1(x_1) \oplus f_1(x_2), ..., f_4(x_1) \oplus f_4(x_2)) \\ &= f(0,0,0,0) \oplus f(1,1,1,1) \end{aligned}$$

and:

$$f(0,0,0,0) \oplus f(1,1,1,1) \oplus f(1,0,0,0) = c$$

Hence, $f(1,0,0,0)$ is known. Send to the oracle plaintext $(1,0,0,0)$, receiving $k \oplus f(1,0,0,0)$.

Therefore, k can be found.