1 Secure PRF

Let \( F : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n \) be a secure PRF (with \( n = 128 \)). Which of the following functions are secure PRFs:

- \( F'(k, x) = F(k, x) \oplus 0 \)
- \( F'(k, x) = k \oplus x \)
- \( F'((k_1, k_2), x) = F(k_1, x) \oplus F(k_2, x) \)
- \( F'(k, x) = \begin{cases} F(k, x) & \text{when } x \neq 0^n \\ 0^n & \text{otherwise} \end{cases} \)
- \( F'((k_1, k_2), x) = F(k_1, x) \oplus F(k_2, x) \)
- \( F'(k, x) = F'(k, x)[0, \ldots, n - 2] \) drops the last bit of \( F(k, x) \)

2 Insecure PRF

Let \( \mathcal{R} = \{0, 1\}^4 \) and consider the function \( F : \mathcal{R}^5 \times R \rightarrow R \), which is computed by the following program:

\[
\begin{align*}
t &= k[0] \\
&\text{for } i = 1 \text{ to } 4 \text{ do} \\
&\quad \text{if } x[i-1] == 1 \text{ then} \\
&\qquad t = t \oplus k[i] \\
&\text{end if} \\
&\text{end for} \\
&\text{output } t
\end{align*}
\]

The key is \( k = (k[0], k[1], k[2], k[3], k[4]) \in \mathcal{R}^5 \). For instance, for the input \( x = 0101 \) the output is \( F(k, x) = F(k, 0101) = k[0] \oplus k[2] \oplus k[2] \oplus k[4] \).

Let \( k \) a random key that unknown. Assume that you learn that

\[
F(k, 0110) = 0011, \quad F(k, 0101) = 1010, \quad F(k, 1110) = 0110.
\]
Determine the value of $F(k, 1101)$ using the above information. Observe that since you are able to predict the function at a new input, this is not a secure PRF.

3 Nonce-based CBC

Recall that if we want to use CBC encryption with a non-random unique nonce, then we must first encrypt the nonce with an independent PRP key and use the result as the CBC IV. Determine what goes wrong if we encrypt the nonce with the same PRP key as the key used for CBC encryption.

Let $F : \mathcal{K} \times \{0, 1\}^\ell \to \{0, 1\}^\ell$ be a secure PRP with $\ell = 128$. Let $n$ be a nonce and suppose we encrypt a message $m$ by first computing $IV = F(k, n)$ and then using this IV in CBC encryption using $F(k, \cdot)$. Observe that the same key $k$ is used for computing the IV and for CBC encryption. The goal is to prove that the resulting system is not nonce-based CPA secure.

The adversary $A$ asks for the encryption of

1. the two block message $m = (0^\ell, 0^\ell)$ with nonce $n = 0^\ell$ and receives a two block ciphertext $(c_0, c_1)$

2. the one block message $m_1 = c_0 \oplus c_1$ with nonce $n = c_0$ and receives a one block ciphertext.

Determine a relation that holds between $c_0$, $c_1$, and $c'_0$ and lets the adversary win the nonce-based CPA game with advantage 1. Explain the derivation of this relation in detail.