CIS5371 – Cryptography **Fall 2025**

Homework 2: Deadline Tuesday 10/28

Instructor: Viet Tung Hoang

1. (50 points) (**A wrong use of AES**) Define the function $F : \{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$ via $F_K(M) = \mathrm{AES}_M(K)$. Note that AES is used incorrectly: the key of F is used as the AES message, and its message as the AES key. Give a key-recovery attack on F using a single query.

2. (70 points) (**A bad variant of Encrypted CBC-MAC**) In class we studied the Encrypted CBC-MAC, where we have a key (K, L). To MAC a message M, we run CBC-MAC on M with subkey L to derive a string V, and then encrypt $T \leftarrow E_K(V)$.

Consider a variant of Encrypted CBC-MAC where $T \leftarrow K \oplus V$, as illustrated in Figure 2.1. This variant is cheaper than Encrypted CBC-MAC, because we replace the last blockcipher call with a one-time pad. However, it's insecure. Break the MAC security of this variant using a few Tag calls.

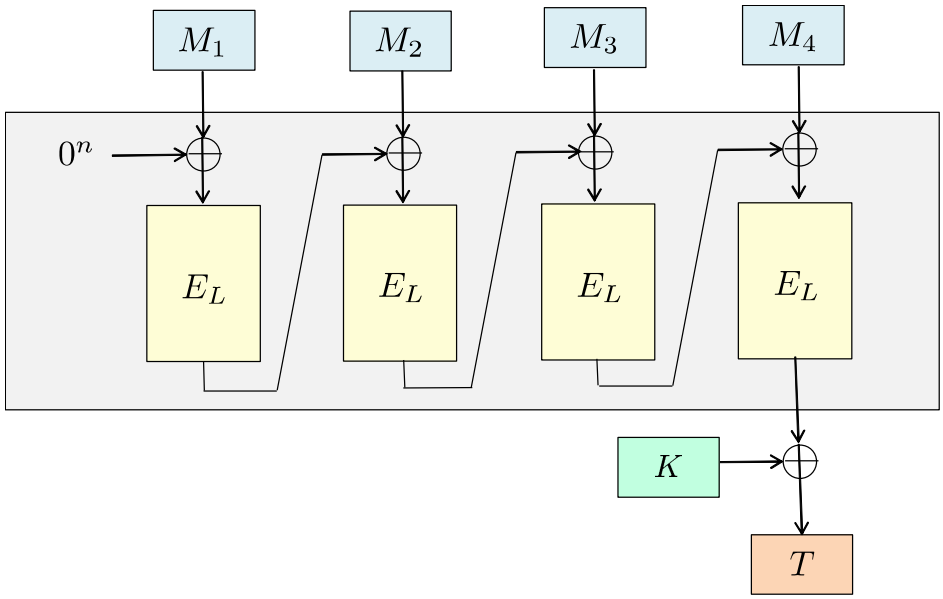

Figure 2.1: A variant of Encrypted CBC-MAC, illustrated for a four-block message $M = M_1M_2M_3M_4$.

3. (60 points) (**A bad variant of CBC ciphertext stealing**) Figure 2.2 below illustrates another way to do ciphertext stealing on CBC with a blockcipher $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$. This variant CBC-S appears in textbooks but is actually *insecure*. (Note that for full-block messages, we still use the standard CBC encryption.) Break the real-or-random security of CBC-S using a few queries and analyze the advantage of your attack.

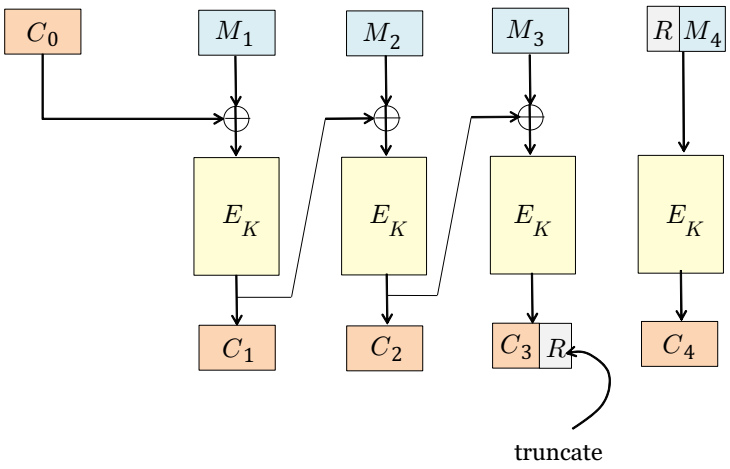

Figure 2.2: A bad variant of ciphertext stealing.