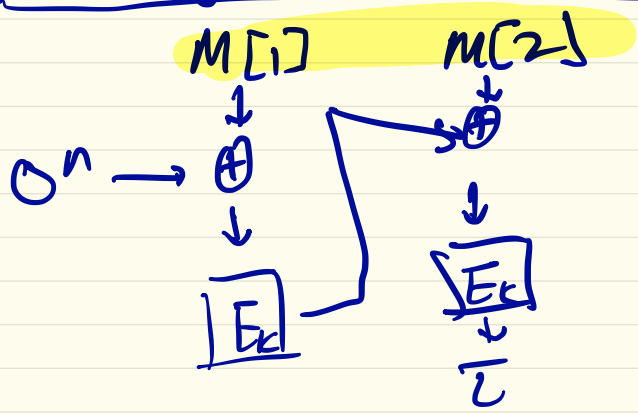
$E: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$

Splicing Attack on CBC



Algorithm F

:

Tag(...)

Tag(...)

return m, T

m not queried to Tag

against plain CBC-MAC

Algorithm F

Let $M_1 \leftarrow \{0,1\}^n$ be arbitrary

$T_1 \leftarrow Tag(M_1)$

$T_2 \leftarrow Tag(0^n)$

Return $(M_1 \| T_1, T_2)$

against ECBC-MAC w/ key reuse.

Algorithm F

$y_1 \leftarrow Tag(1^n)$

$y_2 \leftarrow Tag(y_1)$

Return $(1^n \| 10^{2n}, y_2)$

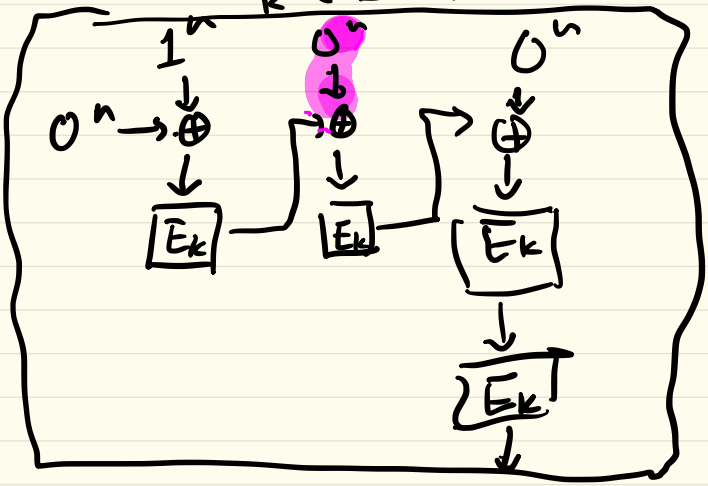
Claim: $Adv^{uf\text{-}cma}_{\mathcal{T}}(F) = 1$.

proof: $y_1 = E_k(E_k(1^n))$

$y_2 = E_k^4(1^n)$

WTS $T_k(1^n \| 10^{2n}) = y_2$

$\tau_k(1^n \| 0^{2n}) =$



picture of computation

$E_k(E_k(E_k(E_k(1^n))))$ ✓

$= y_2$ as desired.

Claim: Resource usage is 2 queries

proof: Looking at the code, [illegible] queries and no [illegible] operations. ✓

$c = (x^z \bmod N, z)$

Algorithm $D_{(p,q)}(c)$:

Parse c as (c_1, z)

$(a, b, 1) \leftarrow EXT-GCD(z, (p-1)(q-1))$

// d is $\gcd(z, (p-1)(q-1))$

// $z \cdot a + (p-1)(q-1) \cdot b = 1$

// $a = z^{-1} \bmod \phi(N)$

return $c^a \bmod N$