# CS409m: Introduction to Cryptography (Aut' 25)

Lecture 11

Instructor: Chethan Kamath

1) **Theorem 3.** If $F$ is a PRF, then construction 1 ($\to M$) is an EU-CMA-secure MAC for fixed-length messages

**Proof.** We proceed by contradiction. Assume there exists an adversary Tam that breaks $\Pi$ with a non-negligible advantage. That is, there exists a polynomial $p$ such that for infinitely-many $n$s,

$$\text{EU-CMA}^{*}_{\text{Tam},M}(1^n) > 1/p(n),$$

where $*$ denotes the probability that Tam breaks $M$ in the EU-CMA game on security parameter $n$. Recall that we assume Tam makes at most $q=q(n)$ Tag queries. We will exploit Tam to design a distinguisher $D$ that breaks $F$'s pseudorandomness. To be specific, we design $D$ such that

$$\left|\Pr_{k}\left[D^{F_k(\cdot)}(1^n)=0\right] - \Pr_{f}\left[D^{f(\cdot)}(1^n)=0\right]\right| > 1/p(n) - 1/2^n.$$

($F_k(\cdot)$: pseudorandom; $f(\cdot)$: random; $O(\cdot)$: either $F_k(\cdot)$ or $f(\cdot)$)

Distinguisher $D^{O(\cdot)}(1^n)$

1) Call Tam$(1^n)$
2) Query phase. For each $i \in [1,q]$:
   a) Tam makes a tag query on $m_i$
   b) Query $O(m_i)$ to obtain $y_i$
   c) Return $t_i := y_i$ as the tag on $m_i$

3) Tam outputs a forgery $t^*$ on $m^*$, such that $m^* \notin \{m_1, \ldots, m_q\}$
4) Query $O(m^*)$ to obtain $y^*$
5) O/p 0 if $t^* = y^*$ and 1 otherwise
(↳ "pseudorandom" ↳ "random")

## Analysis

When $O(\cdot) = F_k(\cdot)$, Tam's view is identical to the EU-CMA experiment and therefore

$$\Pr_k\left[D^{F_k(\cdot)}(1^n) = 0\right] = \text{EU-CMA}_{\text{Tam},M}(1^n) > 1/p(n). \quad \text{—①}$$

On the other hand, when $O = f(\cdot)$, since $f$ is sampled uniformly a random and $m^* \notin \{m_1, \ldots, m_q\}$ we have

$$\Pr\left[t^* = y^*\right] = 1/2^n$$

and thus

$$\Pr_f\left[D^{f(\cdot)}(1^n) = 0\right] = 1/2^n \quad \text{—②}$$

By ① - ②, we get for infinitely many $n$s

$$\left|\Pr_k\left[D^{F_k(\cdot)}(1^n) = 0\right] - \Pr_f\left[D^{f(\cdot)}(1^n) = 0\right]\right| > \left|1/p(n) - 1/2^n\right|,$$

which is non-negligible