CIS 5560

Cryptography
Lecture 13

Announcements

- HW 4 is out, due on Friday
- No HW due for next week, we will provide a worksheet to practice problems

Recap of last lecture

Other properties of (hash) functions

- Collision resistance:
  - Can't find two inputs with same output
  - That is, can't find $x \neq x'$ such that $h(x) = h(x')$
- One-wayness/Preimage resistance:
  - Difficult to find input given an output
  - That is, given $y \in \text{Range}(h)$, can't find x s.t. $h(x) = y$
- 2nd-preimage resistance:
  - Given input x, can't find another input with same output
  - That is, given x, can't find x' s.t. $h(x) = h(x')$

One-way Functions: The Definition

A function (family) $\{F_n\}_{n\in\mathbb{N}}$ where $F(\cdot) : \{0,1\}^n \to \{0,1\}^{m(n)}$ is **one-way** if for every p.p.t. adversary A, the following holds:

$$\Pr\left[F_n(x') = y \;\middle|\; \begin{array}{r} x \leftarrow \{0,1\}^n \\ y := F_n(x) \\ x' \leftarrow A(1^n, y) \end{array}\right] = \text{negl}(n)$$

- Can always find *an* inverse with unbounded time
- … but should be hard with probabilistic polynomial time

One-way Permutations:

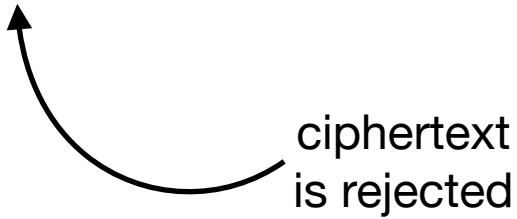
One-to-one one-way functions with $m(n) = n$.

Goals

An **authenticated encryption** system (Gen, Enc, Dec) is a cipher where

As usual: $\text{Enc} : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$

but $\text{Dec} : \mathcal{K} \times \mathcal{C} \to \mathcal{M} \cup \{\text{Error} / \perp\}$

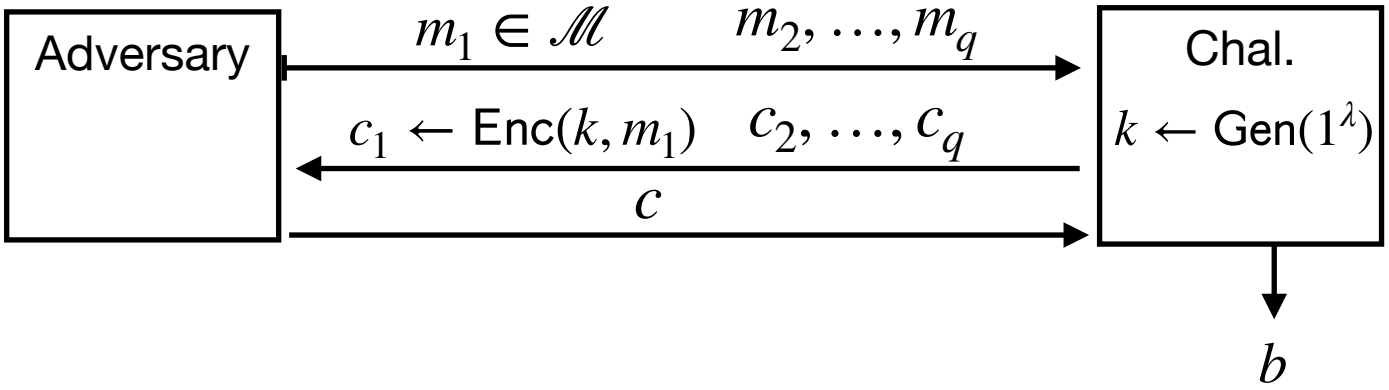


Security: the system must provide

- IND-CPA, and
- **ciphertext integrity:**
  attacker cannot create new ciphertexts that decrypt properly

Ciphertext integrity

Let (Gen, Enc, Dec) be a cipher with message space $\mathcal{M}$.



$b = 1$ if $\text{Dec}(k, c) \neq \perp$ and $c \notin \{c_1, \ldots, c_q\}$

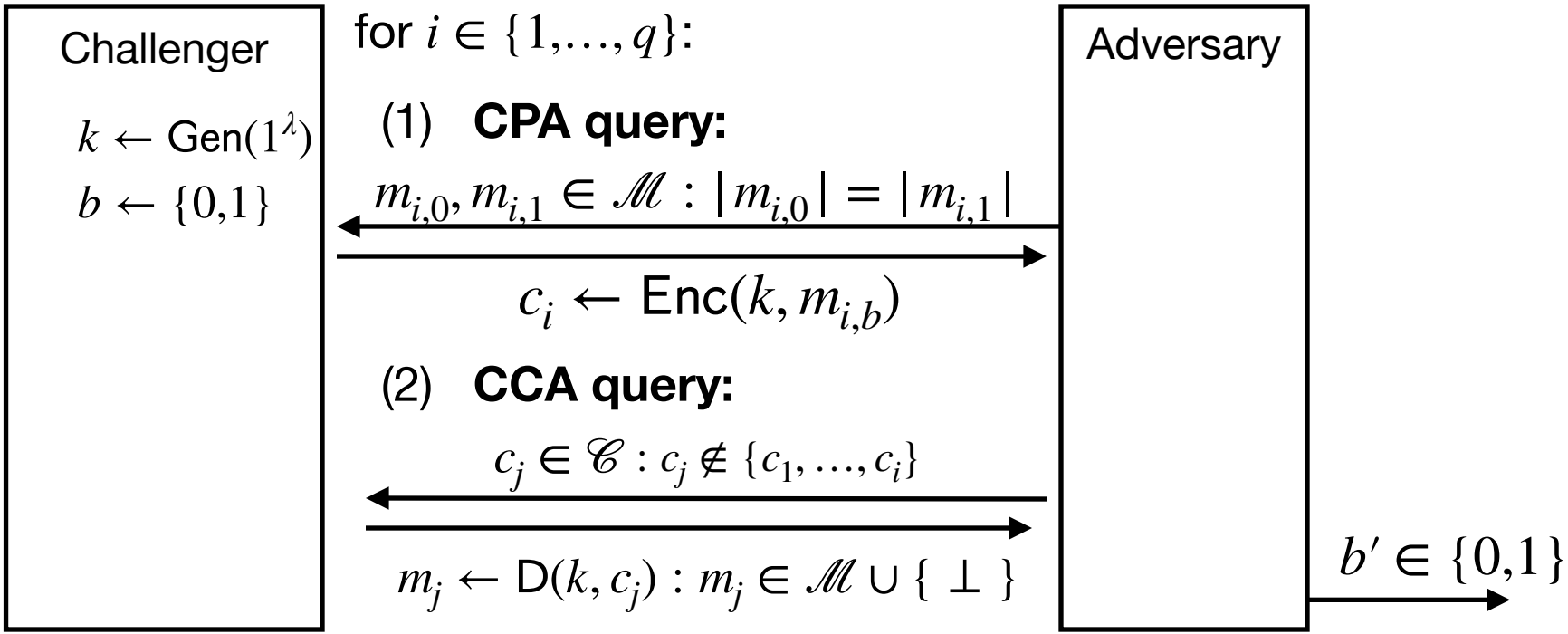
$b = 0$ otherwise

Def: (Gen, Enc, Dec) has **ciphertext integrity** if for all PPT A:

$$\text{Adv}_{\text{CI}}[A] = \Pr[b = 1] = \text{negl}(\lambda)$$

Chosen ciphertext security: definition

Let (Gen, Enc, Dec) be a cipher with message space $\mathcal{M}$



Today

- AE → IND-CCA
- Constructions of AE
- MACs from UHF

Authenticated enc. ⇒ CCA security

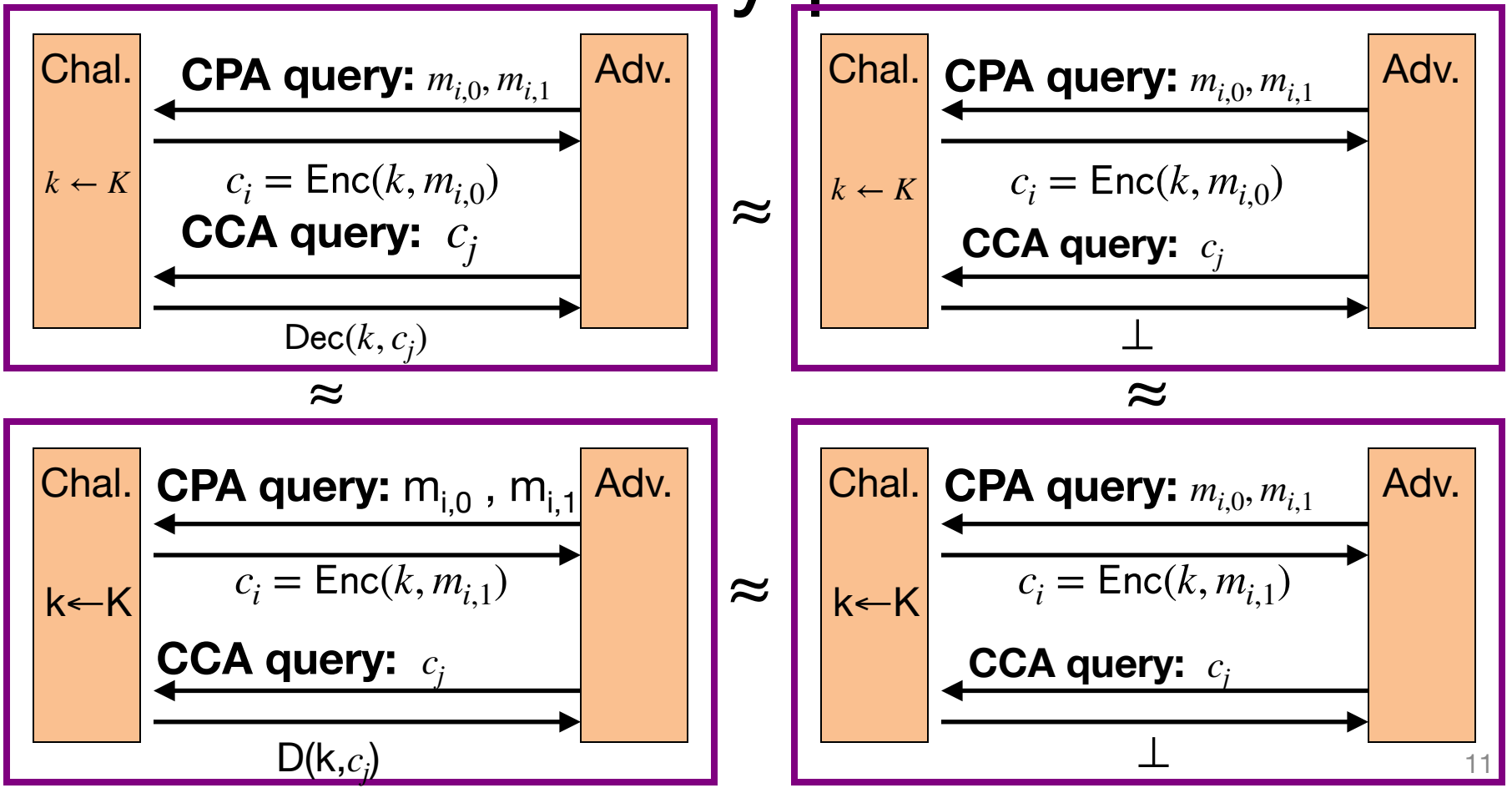
Thm: Let (E,D) be a cipher that provides AE.

Then (E,D) is CCA secure !

In particular, for any q-query eff. A there exist eff. B_1, B_2 s.t.

$$Adv_{CCA}[A,E] \le 2q \cdot Adv_{CI}[B_1,E] + Adv_{CPA}[B_2,E]$$

Proof by pictures



So what?

Authenticated encryption:

- ensures confidentiality against an active adversary that can decrypt some ciphertexts

Limitations:

- does not prevent replay attacks
- does not account for side channels (timing)

Constructions of AE

… but first, some history

Authenticated Encryption (AE): introduced in 2000 [KY'00, BN'00]

Crypto APIs before then:

- Provide API for CPA-secure encryption (e.g. CBC with rand. IV)
- Provide API for MAC (e.g. HMAC)

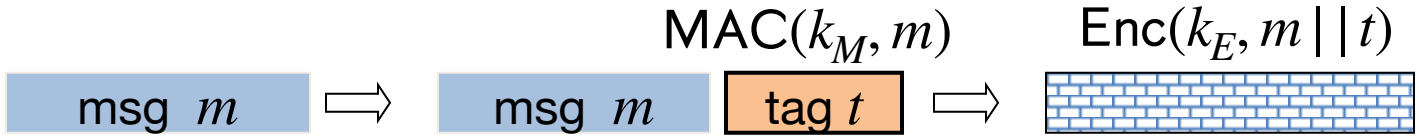
Every project had to combine the two itself without a well defined goal

- Not all combinations provide AE …

Combining MAC and ENC (CCA)

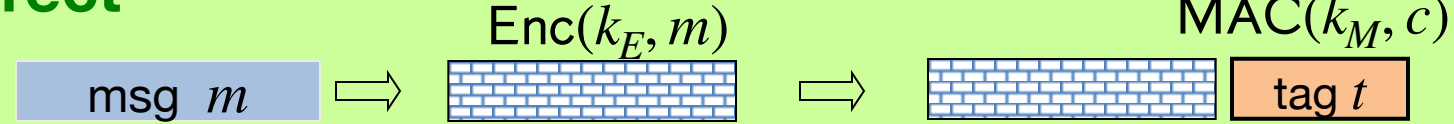
Encryption key k_E. MAC key = k_M

Option 1: (SSL)

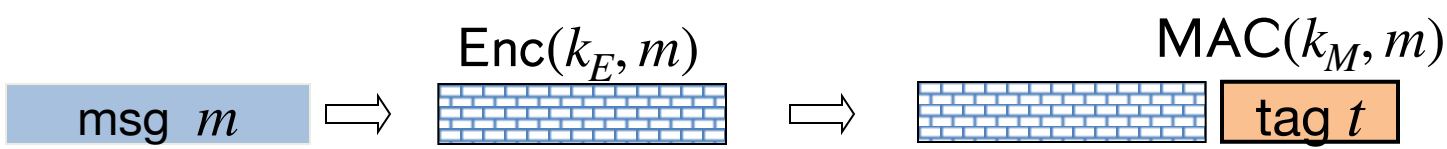


always correct

Option 2: (IPsec)



Option 3: (SSH)



A.E. Theorems

Let (E,D) be CPA secure cipher and (S,V) secure MAC.
Then:

1. **Encrypt-then-MAC**: always provides A.E.

2. **MAC-then-encrypt**: may be insecure against CCA attacks

   however: when (E,D) is rand-CTR mode or rand-CBC
   M-then-E provides A.E.

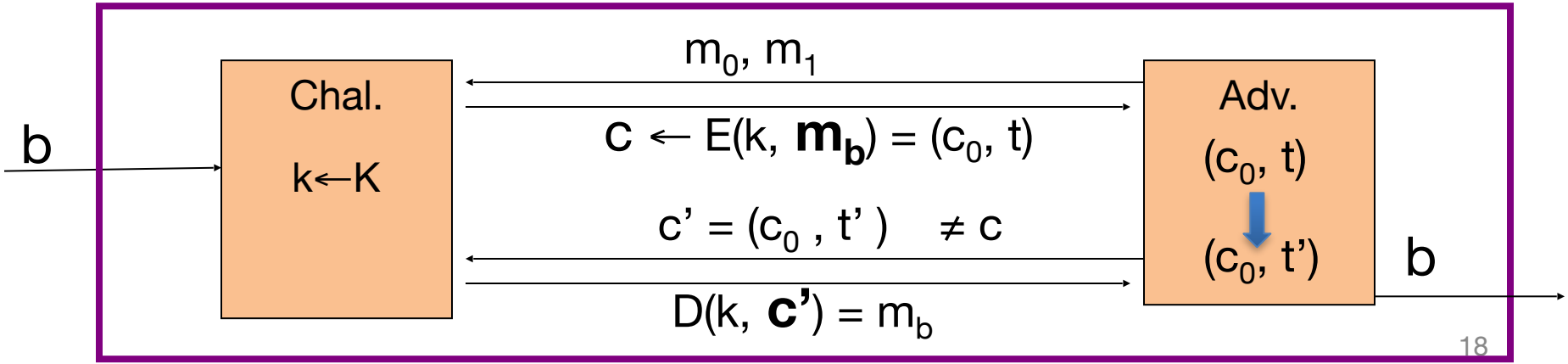
Security of Encrypt-then-MAC

Security of Encrypt-then-MAC

Recall: MAC security says that you can't generate new message-tag pairs

Here the "message" is the (unauthenticated) ciphertext, and "tag" is the MAC tag.

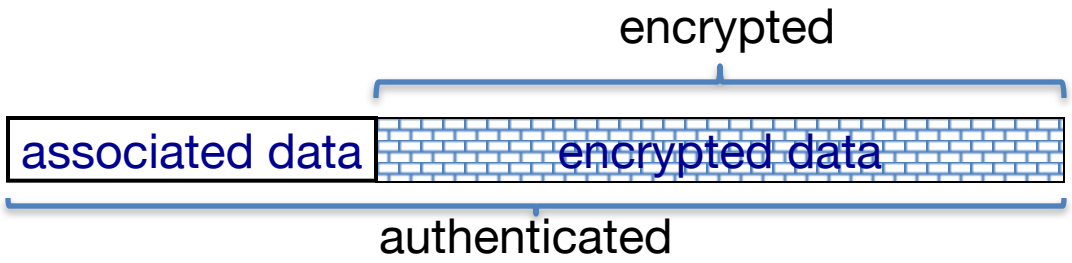
So MAC security says that we can generate new (c, t) pair, but this is exactly a ciphertext for the AE scheme! So MAC security → ciphertext integrity for AE.



Standards (at a high level)

- **GCM**: CTR mode encryption then CW-MAC
  (accelerated via Intel's PCLMULQDQ instruction)
- **CCM**: CBC-MAC then CTR mode encryption (802.11i)
- **EAX**: CTR mode encryption then CMAC

All support AEAD: (auth. enc. with associated data). All are nonce-based.



AES-GCM

- **GCM:** **CTR mode encryption then CW-MAC**
  (accelerated via Intel's PCLMULQDQ instruction)
- **CCM**: CBC-MAC then CTR mode encryption (802.11i)
- **EAX**: CTR mode encryption then CMAC

Universal Hashes

- We have seen MACs from PRFs and from CRHFs
- However, the fastest kind of MAC, and the one used in AES-GCM, takes a third, different, approach.
- It constructs MACs from *universal hash functions (UHF).*
- A UHF is similar to a CRHF, except that it relies on a key:

  for *all* adversaries A, the following probability is negligible:

$$Pr_{k \leftarrow \mathcal{K}}[H(k,m) = H(k,m') \mid (m,m') \leftarrow A] = \mathsf{negl}()$$

Simplest UHF

- The simplest UHF is defined based on polynomials modulo a prime as follows.
- Let p be a large prime.
- Our message space will be $\mathbb{Z}_p^{\ell+1}$ for some ℓ
- The hash function is defined as follows:

$$H(k, m = (m_0, \ldots, m_\ell)) \\ := m_0 \cdot k^0 + m_1 \cdot k^1 + m_2 \cdot k^2 + \cdots + m_\ell \cdot k^\ell$$

Simplest UHF

- How hard is to find collisions?
- Consider two message a, b.

$$H(k, a) = H(k, b)$$

$$\sum_i a_i k^i = \sum_i b_i k^i$$

$$\sum_i (a_i - b_i) k^i = 0$$

- This expression is 0 when k is a root of the polynomial coefficients $a_i - b_i$
- What is the probability of this happening for uniformly chosen k?
- Answer: just ℓ / p! If p is large and ℓ is polynomial sized, this is negligible.

UHF + small PRF → big PRF

- Recall: CRH + PRF for short messages → PRF for long messages
- We can apply the same idea here: UHF + PRF for short messages → PRF for long messages
- Let H be UHF, F be PRF.
- Then $F'(k = (k_H, k_F), m) := F(k_F, H(k_H, m))$ is a secure PRF.
- Idea: if we could find messages (m, m') with same hash, then evaluation of F' on (m, m') would be equal. This distinguishes F' from a random function.
- However, UHF property of H prevents this.