https://class.coursera.org/crypto-preview/class/index

MÃ XÁC THỰC THÔNG ĐIỆP

- *Toàn vẹn thông điệp*
- *MAC dựa trên PRF*
- *CBC-MAC và NMAC*
- *MAC padding*

MÃ XÁC THỰC THÔNG ĐIỆP

- *Toàn vẹn thông điệp*
- *MAC dựa trên PRF*
- *CBC-MAC và NMAC*
- *MAC padding*

https://class.coursera.org/crypto-preview/class/index

Toàn vẹn thông điệp

Mục đích

- Toàn vẹn, không cần bí mật

Ví dụ

- Bảo vệ các file công khai trên đĩa
- Bảo vệ các banner quảng cáo trên trang web

Toàn vẹn thông điệp: MAC (Message Authentication Code)

Định nghĩa. MAC $I = (S, V)$ định nghĩa trên (K, M, T) là một cặp thuật toán:

- $S(k, m)$ output t thuộc T
- $V(k, m, t)$ output 'yes' hoặc 'no'

Toàn vẹn thông điệp cần một khóa bí mật

- Kẻ tấn công có thể dễ dàng thay đổi thông điệp và tính lại CRC (Cyclic redundancy check).

- CRC được thiết kế để phát hiện lỗi xảy ra ngẫu nhiên chứ không chống được lỗi có chủ đích.

MAC an toàn

Khả năng của kẻ tấn công

- kẻ tấn công có thể lấy được các tag $t_i \leftarrow S(k, m_i)$ của $m_1, m_2, \ldots, m_q$

Mục đích của kẻ tấn công: Giả mạo thông điệp

- đưa ra được một cặp thông điệp/tag (m, t) hợp lệ mới

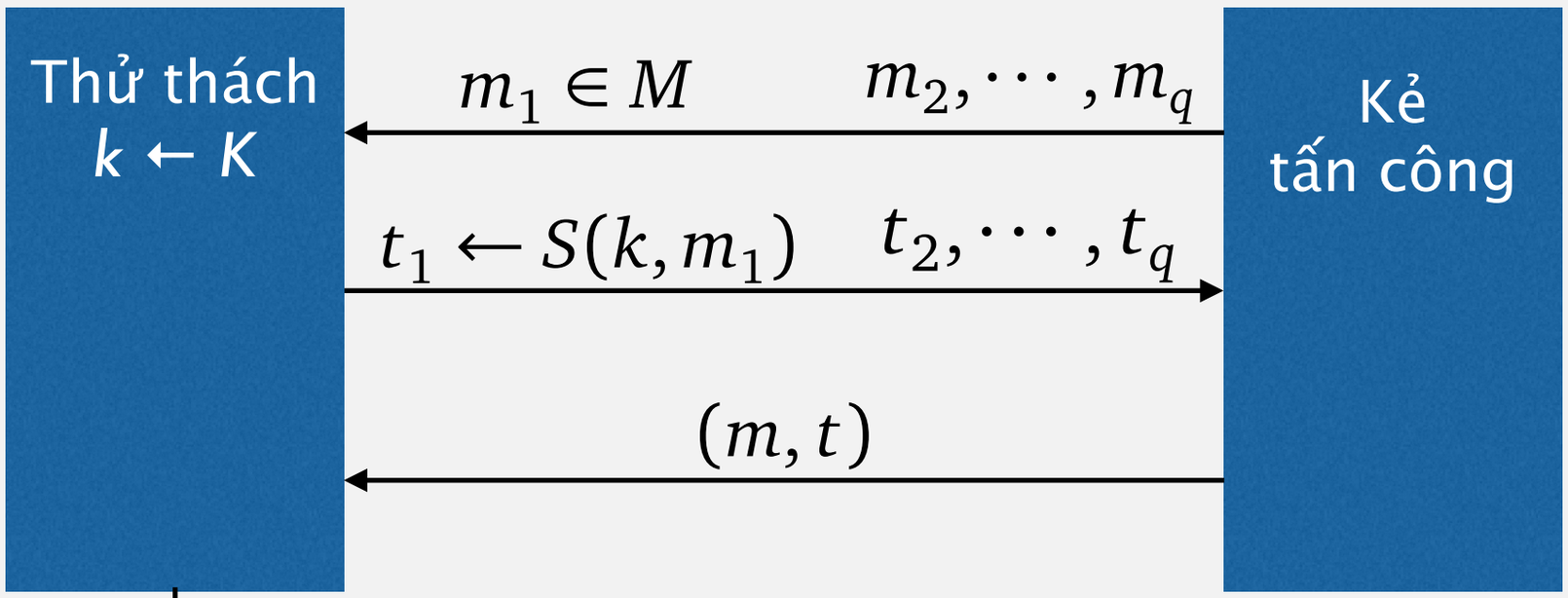
$$(m, t) \notin \{(m_1, t_1), \cdots, (m_q, c_q)\}$$

Có nghĩa rằng:

- kẻ tấn công không thể tạo ra một tag hợp lệ cho một thông điệp mới
- đưa ra (m, t) kẻ tấn công thậm chí không tạo được (m, t') với $t' \neq t$

MAC an toàn

Cho MAC $I = (S, V)$ và một kẻ tấn công A. Ta định nghĩa một thử nghiệm MAC như sau:



$$\begin{cases} b = 1 & \text{nếu } V(k, m, t) = \text{'yes' và } (m, t) \notin \{(m_1, t_1), \cdots, (m_q, t_q)\} \\ b = 0 & \text{ngược lại} \end{cases}$$

Định nghĩa. MAC $I = (S, V)$ là MAC an toàn nếu với mọi thuật toán "hiệu quả " A:

$\text{Adv}_{\text{MAC}}[A, I] = \Pr[\text{Thử thách output} = 1]$ là "không đáng kể"

Câu hỏi

Xét *I*=(*S*,*V*) là một MAC.

Giả sử một kẻ tấn công có thể tìm được $m_0 \neq m_1$ sao cho

$$S(k, m_0) = S(k, m_1)$$ với 1/2 số khóa *k* trong K.

Vậy MAC này có an toàn không?

1. Có, kẻ tấn công không thể sinh tag đúng cho m_0 hoặc m_1
2. Không, MAC này có thể bị phá dùng tấn công chọn thông điệp
3. Nó phụ thuộc vào thiết kế của MAC

Câu hỏi

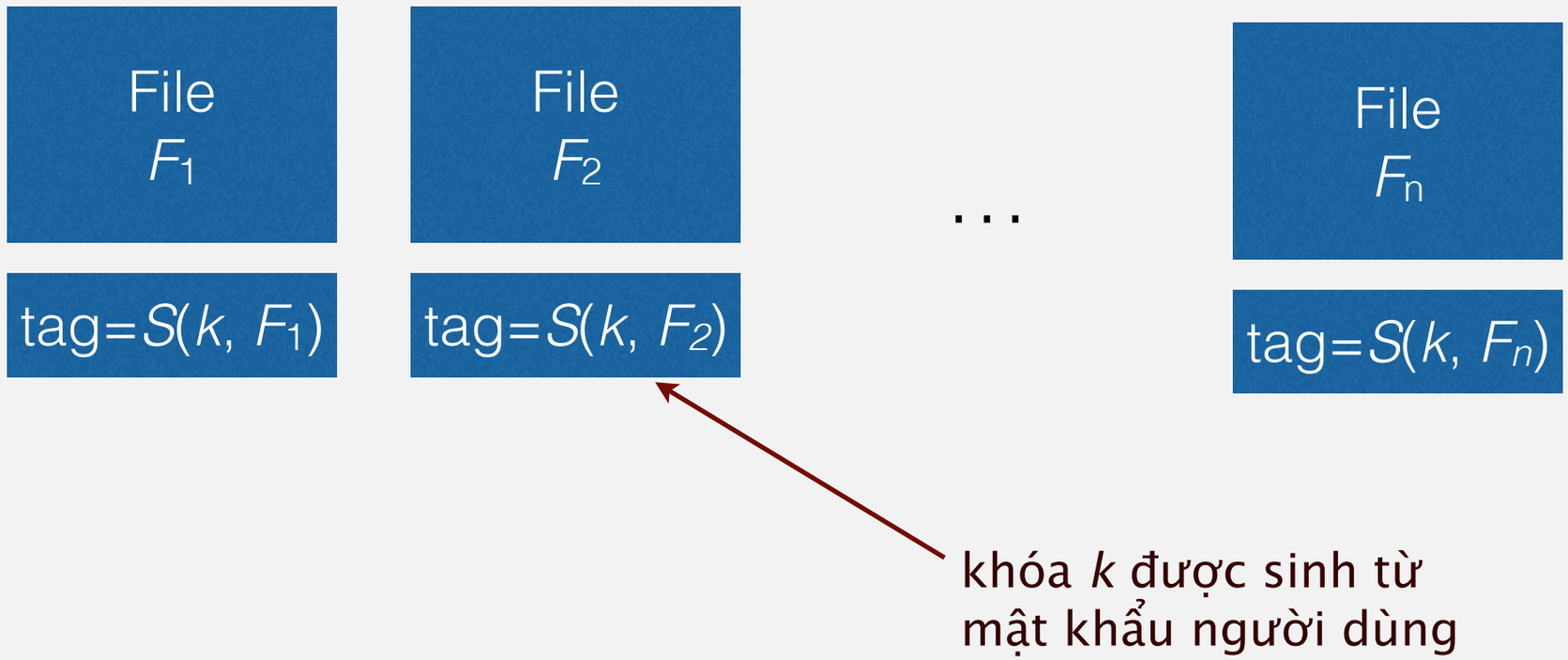
Xét MAC $I=(S,V)$ và giả sử $S(k,m)$ luôn output dãy 5 bit.

MAC này có an toàn không?

1. Không, kẻ tấn công có thể gợi ý tag cho các thông điệp
2. Nó phụ thuộc vào thiết kế chi tiết của MAC
3. Có, kẻ tấn công không thể sinh tag hợp lệ cho bất kỳ thông điệp nào.

Ví dụ: Bảo vệ hệ thống files

Giả sử tại thời điểm cài đặt hệ thống tính toán:



Sau đó hệ thống bị nhiễm virus, và các file bị sửa đổi.

Người dùng khởi động lại vào OS sạch và nhập mật khẩu

- Khi đó: MAC an toàn sẽ cho phép phát hiện các file bị sửa đổi

MÃ XÁC THỰC THÔNG ĐIỆP

- *Toàn vẹn thông điệp*
- *MAC dựa trên PRF*
- *CBC-MAC và NMAC*
- *MAC padding*
- *PMAC và Carter-Wegman MAC*

https://class.coursera.org/crypto-preview/class/index

Hàm giả ngẫu nhiên

Hàm giả ngẫu nhiên (PRF) định nghĩa trên (K, X, Y) là hàm:

$$F: K \times X \rightarrow Y$$

thỏa mãn có thuật toán "hiệu quả" để tính $F(k,x)$

PRF và hàm ngẫu nhiên

Ta ký hiệu

$$\text{Funs}[X, Y] := \{ \text{mọi hàm từ } X \text{ lên } Y \}$$

Câu hỏi: Lực lượng của $\text{Funs}[X, Y]$?

Cho trước một PRF $F: K \times X \rightarrow Y$ ta đặt

$$S_F := \{F(k,.) \text{ thỏa mãn } k \in K\}$$

Câu hỏi: Lực lượng của S_F ?

PRF an toàn: trực giác

Một PRF *F* là an toàn nếu ta không thể phân biệt được một hàm được lấy ngẫu nhiên từ Funs[X,Y] hay lấy ngẫu nhiên từ S_F

PRF an toàn trong thực tế

- 3DES: $\{0,1\}^{168} \times \{0,1\}^{64} \rightarrow \{0,1\}^{64}$
- AES128:$\{0,1\}^{128} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$

Nhắc lại: MAC an toàn

MAC:

- Thuật toán ký: $t \leftarrow S(k, m)$
- Thuật toán kiểm tra: $V(k,m,t)$ = ‘yes’ hoặc ‘no’

Khả năng của kẻ tấn công

- kẻ tấn công có thể lấy được các tag $t_i \leftarrow S(k, m_i)$ của $m_1, m_2,\ldots,m_q$

Mục đích của kẻ tấn công: Giả mạo thông điệp

- đưa ra được một cặp thông điệp/tag (m, t) hợp lệ mới

$$(m, t) \notin \{(m_1, t_1), \cdots, (m_q, c_q)\}$$

Kẻ tấn công không thể tạo tag hợp lệ cho một thông điệp mới

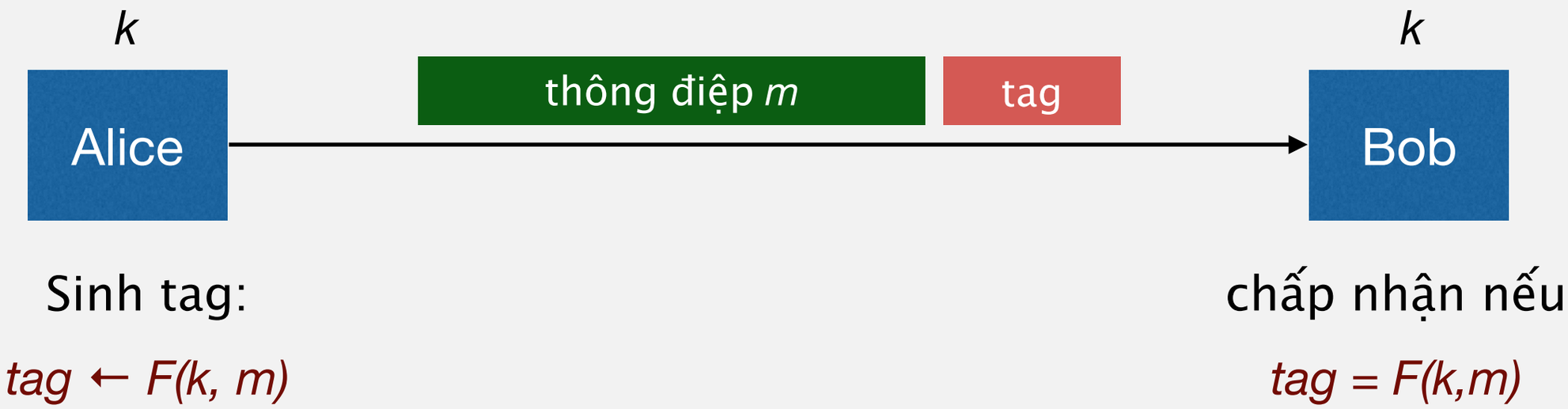
MAC an toàn từ PRF an toàn

Xét PRF $F : K \times X \rightarrow Y$ ta định nghĩa MAC

$$I_F = (S, V)$$

bởi

- $S(k, m) := F(k, m)$
- $V(k, m, t) :=$ [‘yes’ nếu $t = F(k,m)$; ’no’ nếu ngược lại]



Câu hỏi

Giả sử $F : K \times X \rightarrow Y$ là một PRF an toàn với $Y=\{0,1\}^{10}$.

MAC I_F có phải là hệ MAC an toàn ?

1. Có, MAC là an toàn vì PRF là an toàn.
2. Không, độ dài tag quá ngắn: người ta có thể gợi ý ngẫu nhiên tag cho thông điệp bất kỳ.
3. Phụ thuộc vào thiết kế chi tiết của hàm F .

Ví dụ: AES là một MAC với thông điệp độ dài 16 byte.

Câu hỏi: làm thế nào chuyển từ MAC nhỏ sang MAC lớn?

Trả lời: Có hai cách xây dựng được dùng trong thực tế.

- CBC-MAC (Ngân hàng - ANSI X9.9, X9.19, FIPS 186-3)
- HMAC (Giao thức cho Internet: SSL, IPSec, SSH,…)

Cả hai cách này đều chuyển từ một PRF nhỏ thành PRF-lớn.

Chặt bớt MAC dựa trên PRF

Bổ đề dễ. Giả sử $F : K \times X \rightarrow \{0,1\}^n$ là một PRF an toàn. Vậy thì

$$F_t(k, m) := F(k, m)[1 \ldots t] \quad \text{với mọi} \quad 1 \leq t \leq n$$

cũng là PRF an toàn.

Hệ quả. Nếu (S, V) là một MAC dựa trên PRF an toàn với output là tag độ dài n-bit, vậy thì MAC bị cắt chỉ lấy w bit cũng là an toàn khi $1/2^w$ là "không đáng kể" (Ví dụ, $w \geq 64$).

MÃ XÁC THỰC THÔNG ĐIỆP

- *Toàn vẹn thông điệp*
- *MAC dựa trên PRF*
- *CBC-MAC và NMAC*
- *MAC padding*

https://class.coursera.org/crypto-preview/class/index

MAC và PRF

Nhắc lại:

- PRF an toàn $F \Rightarrow$ MAC an toàn, khi $|Y|$ lớn.
- Cách xây dựng: $S(k, m) = F(k, m)$

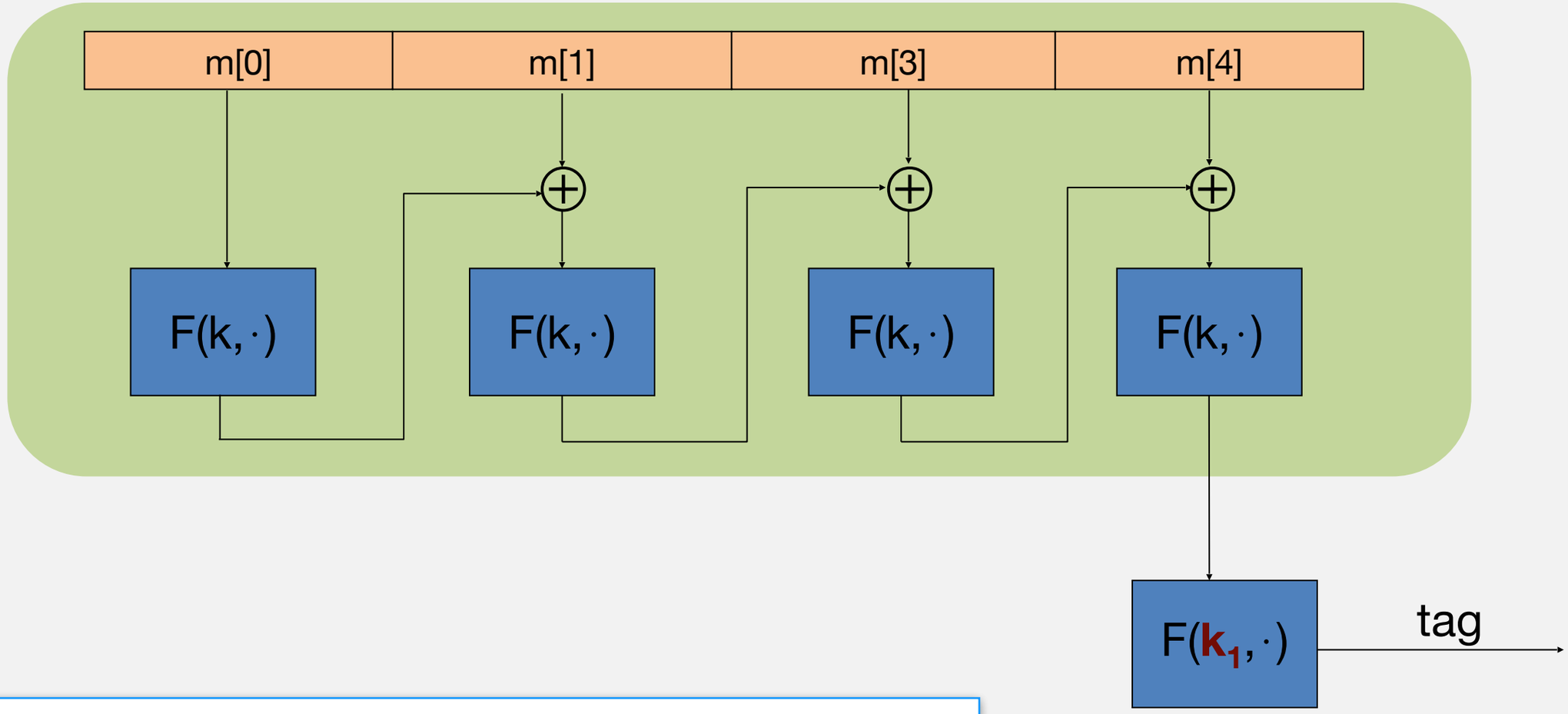
Mục đích của chúng ta:

- Từ PRF cho thông điệp ngắn (Ví dụ AES), tìm cách xây dựng PRF cho thông điệp dài tùy ý.

Xây dựng 1: ECBC-MAC

(CBC-MAC được mã hóa)

raw CBC

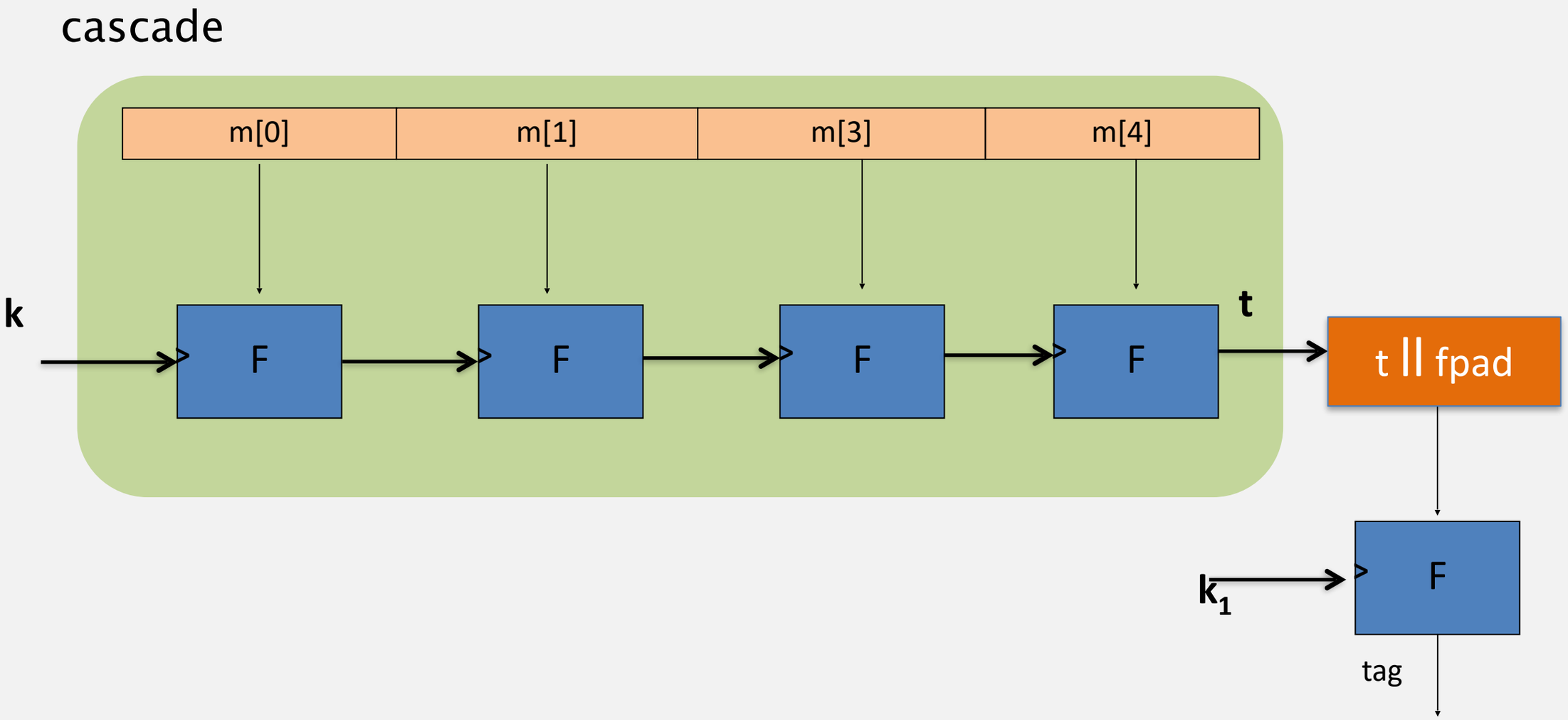


Xét F: K x $X \longrightarrow X$ là PRF.

Ta định nghĩa PRF:

$$F_{ECBC} : K^2 \times X^{\leq L} \rightarrow X$$

Xây dựng 2: NMAC (nested MAC)



Xét F: $K \times X \longrightarrow K$ là PRF.

Ta định nghĩa PRF:

$$F_{\text{NMAC}} : K^2 \times X^{\leq L} \rightarrow K$$

Tại sao trong bước cuối của ECBC-MAC và NMAC phải mã hóa?

NMAC. Giả sử ta định nghĩa MAC $I = (S, V)$ với

$$S(k, m) = \text{cascade}(k,m)$$

1. MAC này là an toàn.
2. MAC này có thể bị giả mạo mà không cần truy vấn bất kỳ thông điệp nào.
3. MAC này có thể bị giả mạo bằng cách truy vấn một thông điệp.
4. MAC này có thể bị giả mạo chỉ bằng truy vấn hai thông điệp.

Tại sao trong bước cuối của ECBC-MAC phải mã hóa?

Giả sử ta định nghĩa MAC $I_{RAW} = (S, V)$ với

$$S(k, m) = \text{rawCBC}(k, m)$$

Vậy thì I_{RAW} có thể bị phá dễ dàng dùng tấn công chọn 1 thông điệp.

Kẻ tấn công thực hiện:

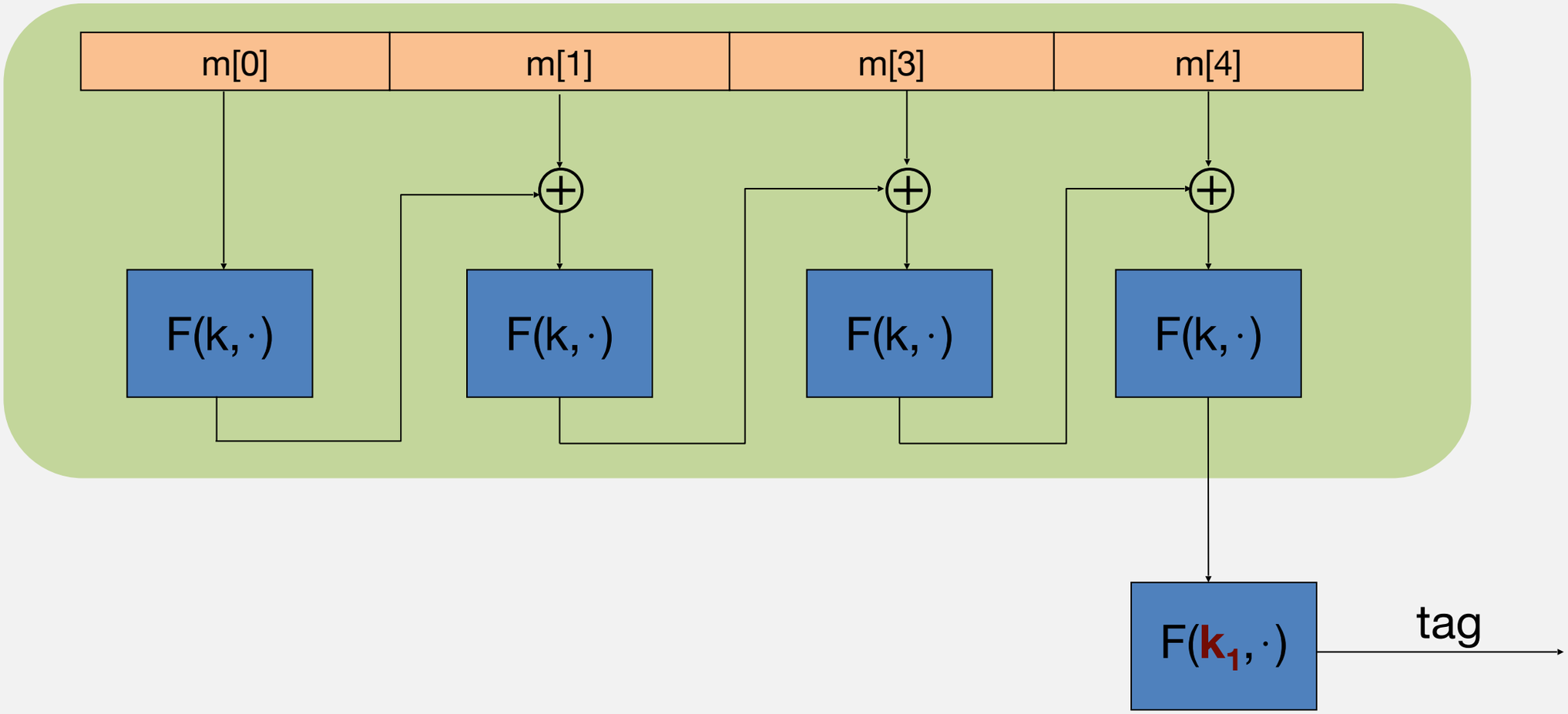
- Chọn một thông điệp chỉ một khối $m \in X$.
- Truy vấn để lấy tag cho m. Anh ta được $t = F(k, m)$.
- Output t như một MAC giả cho thông điệp gồm 2 khối $(m, t \oplus m)$.

Thật vậy,

$$\text{rawCBC}(k, (m,\ t \oplus m)) = F(k, F(k, m) \oplus (t \oplus m)) = F(k, t \oplus (t \oplus m)) = \text{t}$$

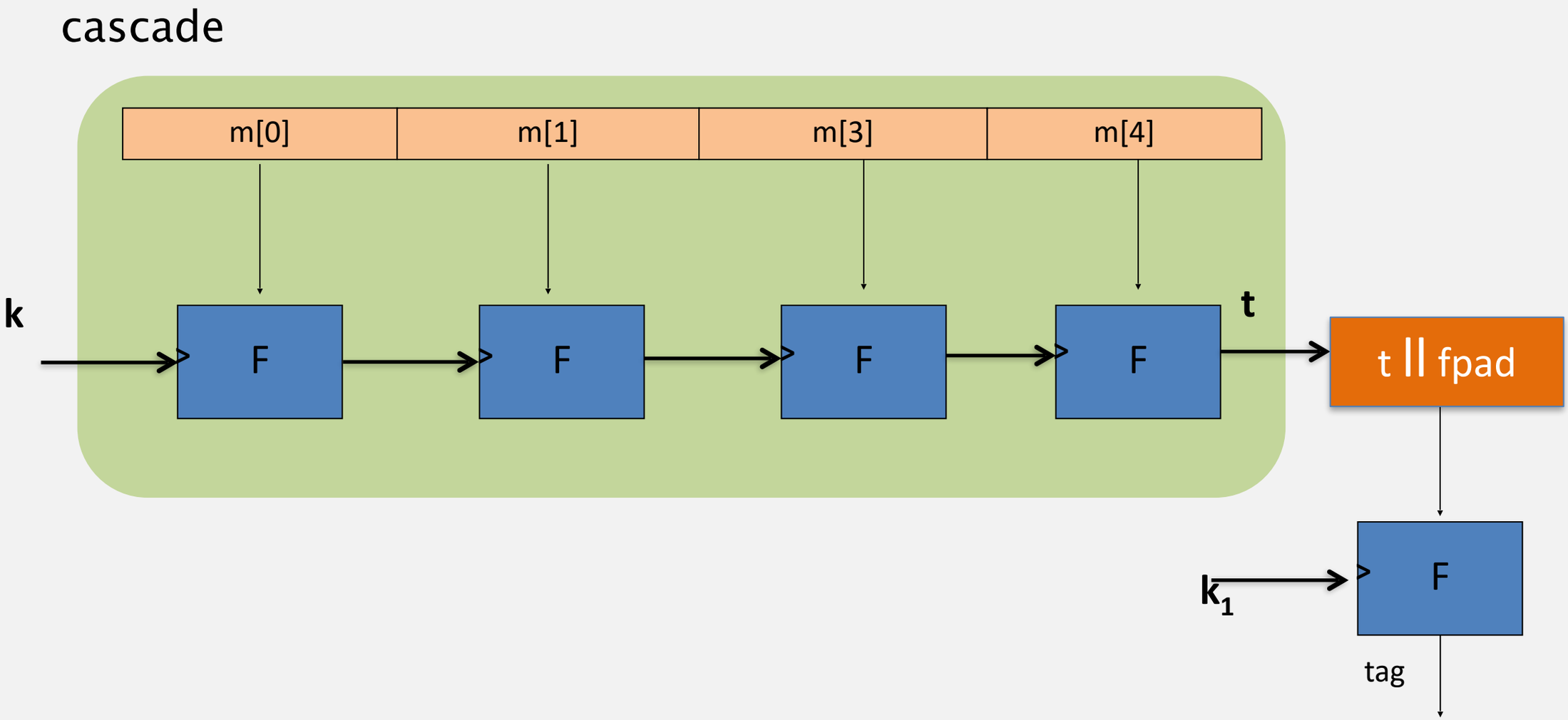
Tính chất mở rộng của ECBC-MAC

raw CBC



$$\forall x, y, w: \quad F_{ECBC}(k, x) = F_{ECBC}(k, y) \quad \Rightarrow \quad F_{ECBC}(k, x \| w) = F_{ECBC}(k, y \| w)$$

Tính chất mở rộng của NMAC (nested MAC)



$$\forall x, y, w: \quad F_{NMAC}(k, x) = F_{NMAC}(k, y) \quad \Rightarrow \quad F_{NMAC}(k, x \| w) = F_{NMAC}(k, y \| w)$$

Tấn công MAC có tính chất mở rộng

Cho PRF $F_{BIG}: K \times X \longrightarrow Y$ be có tính chất mở rộng:

$$\forall x, y, w: \quad F_{BIG}(k, x) = F_{BIG}(k, y) \quad \Rightarrow \quad F_{BIG}(k, \ x \| w) = F_{BIG}(k, y \| w)$$

MAC xây dựng từ PRF trên có thể bị tấn công theo thuật toán sau:

Bước 1: gửi $|Y|^{1/2}$ truy vấn ngẫu nhiên cho các thông điệp trong X.

đạt được (m_i, t_i) for $i = 1, \ldots, |Y|^{1/2}$

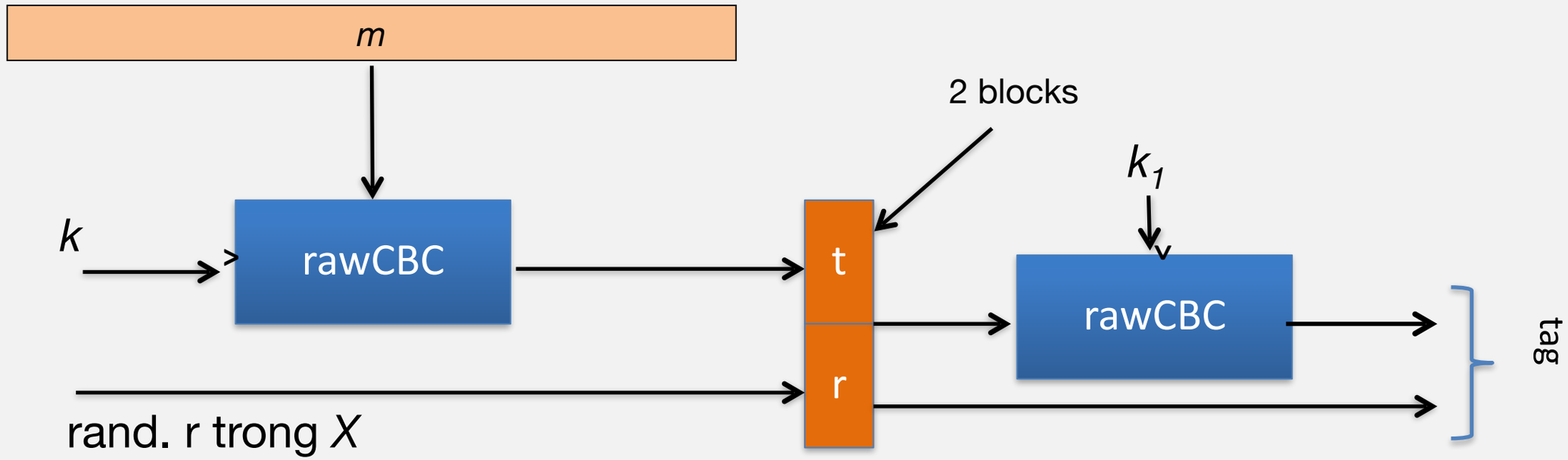
Bước 2: tìm một xung đột $t_u = t_v$ for $u \neq v$ (với xác suất cao là tìm được theo nghịch lý ngày sinh)

Bước 3: chọn một w và truy vấn để lấy $t := F_{BIG}(k, \boldsymbol{m_u \| w})$

Bước 4: đưa ra cặp giả mạo $(m_v \| w, t)$.

Thật vậy $t := F_{BIG}(k, m_v \| w)$.

Sơ đồ an toàn hơn: Xây dựng ngẫu nhiên RCBC



- PRF: $F: K \times X \longrightarrow X$
- Kết quả: MAC với tag trong X^2

So sánh

ECBC-MAC thường dùng là MAC dựa trên AES

- Mode mã hóa CCM (dùng trong 802.11i)
- Chuẩn NIST gọi là CMAC

NMAC thường không dùng với AES hoặc 3DES

- Lý do chính: phải đổi khóa AES trên mọi block ⇒ phải tính lại AES key expansion.
- Nhưng NMAC là cơ sở cho MAC được dùng phổ biên là HMAC.

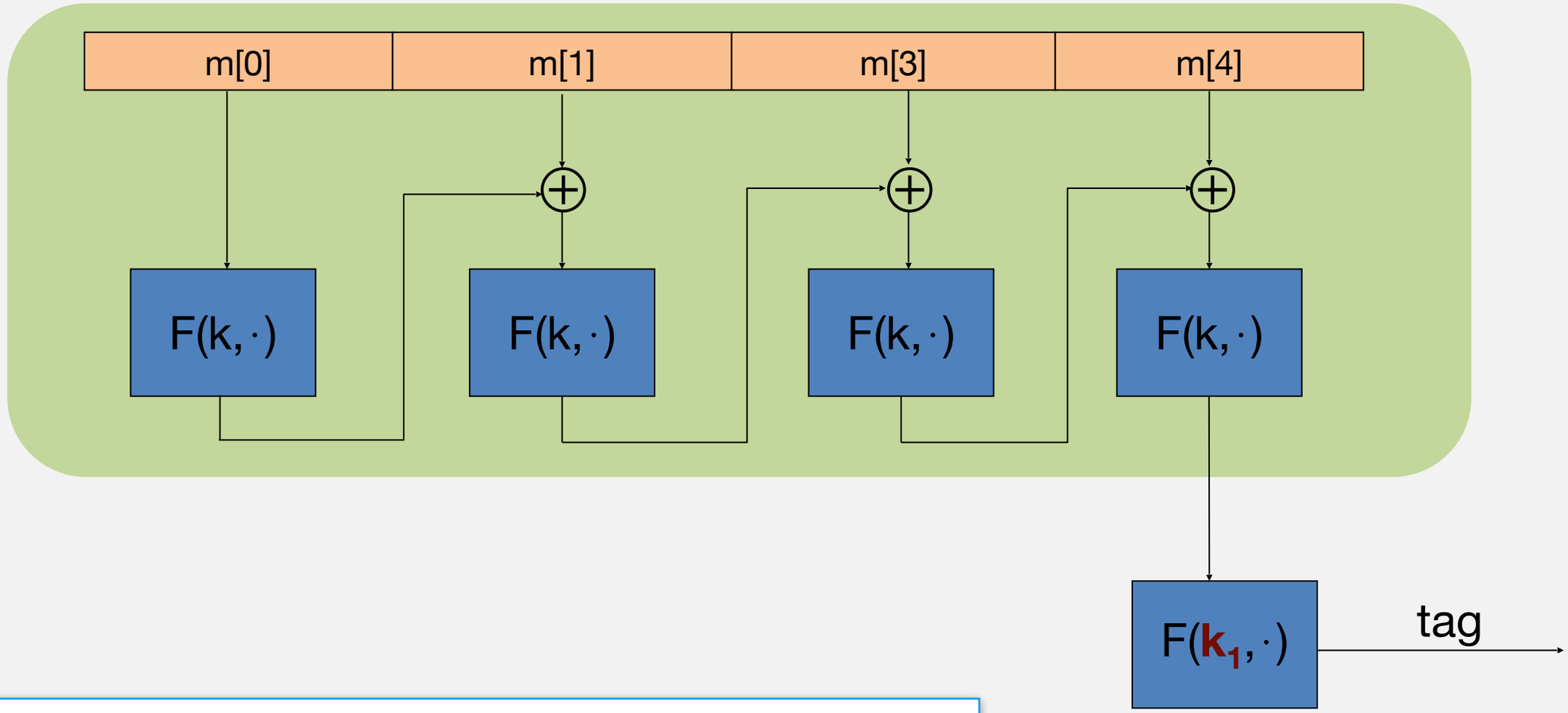
MÃ XÁC THỰC THÔNG ĐIỆP

- *Toàn vẹn thông điệp*
- *MAC dựa trên PRF*
- *CBC-MAC và NMAC*
- *MAC padding*

https://class.coursera.org/crypto-preview/class/index

Nhắc lại: ECBC-MAC

raw CBC

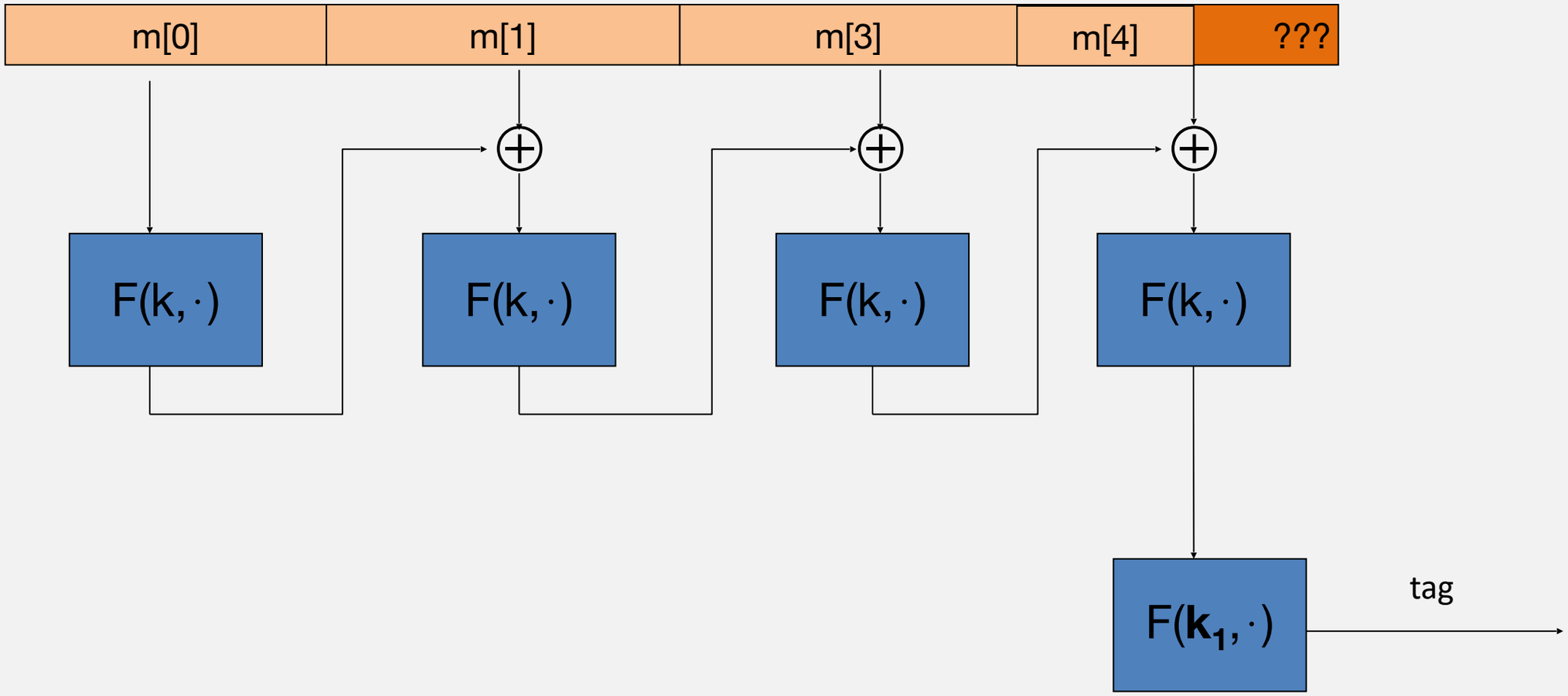


Xét F: K x $X \longrightarrow X$ là PRF.

Ta định nghĩa PRF:

$$F_{ECBC} : K^2 \times X^{\leq L} \rightarrow X$$

Nếu kích thước thông điệp không là bội của block-size thì sao?



CBC MAC padding

Ý tưởng ngây thơ: pad *m* với dãy 0

Câu hỏi. MAC thu được có an toàn?

1. Có, MAC này an toàn.
2. Còn phụ thuộc vào thiết kế chi tiết của MAC.
3. Không, nếu lấy được tag của *m*, kẻ tấn công cũng lấy được tag của *m*||0.

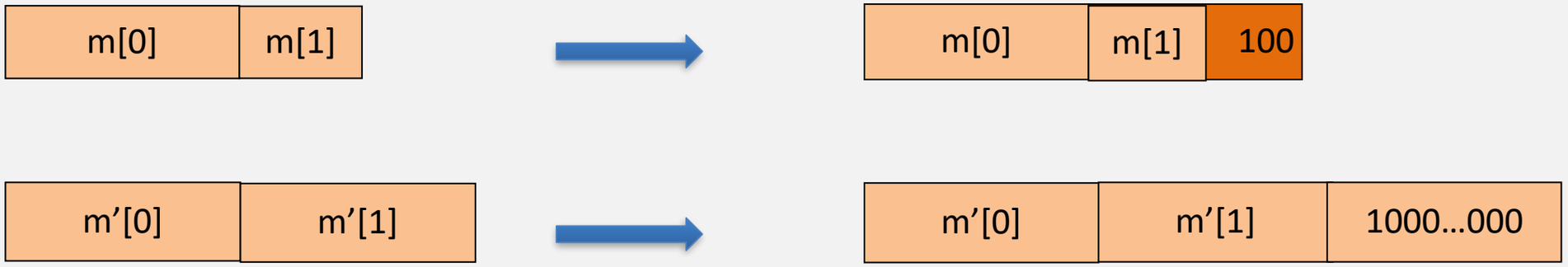
CBC MAC padding

Để an toàn, padding phải khả nghịch, tức là:

$$m_0 \neq m_1 \quad \Rightarrow \quad \text{pad}(m_0) \neq \text{pad}(m_1)$$

ISO. pad với “1000…00”. Thêm block giả nếu cần.

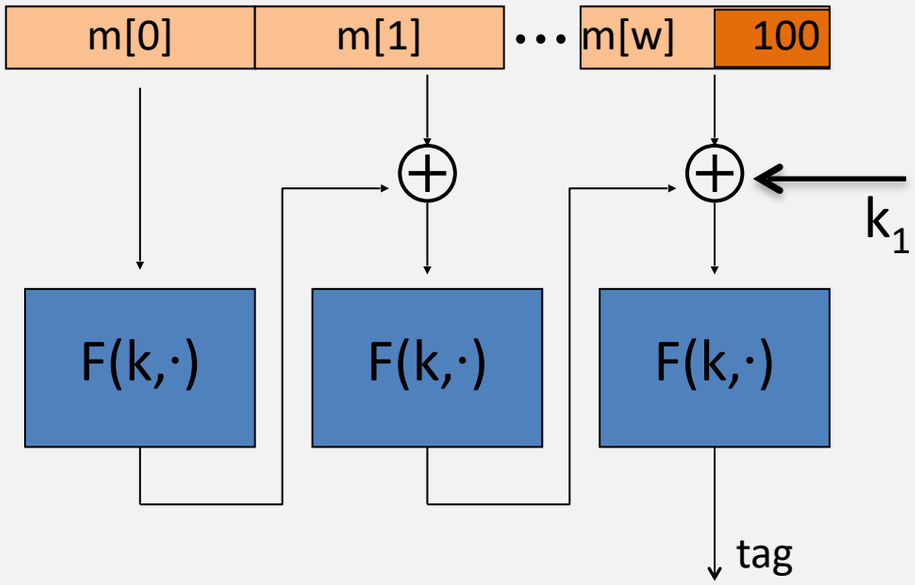
- Số ‘1’ chỉ ra vị trí bắt đầu của pad.

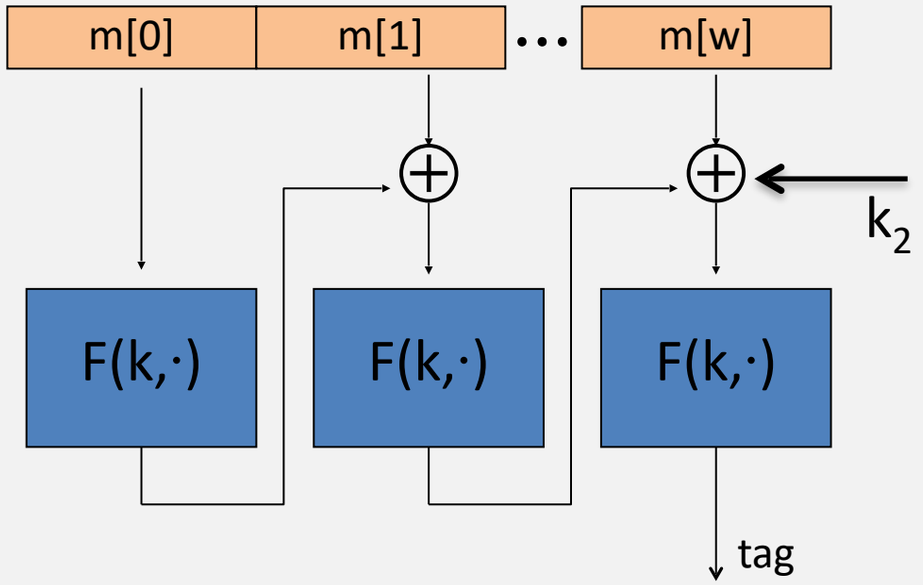


CMAC (Chuẩn NIST)

Là một biến thể của ECBC-MAC: với key = (k, k_1,k_2)

- Không cần bước mã hóa cuối (tấn công mở rộng bị chặn bằng cách *xor* với khóa cuối)
- Không cần block giả (nhập nhằng được loại bỏ bằng cách sử dụng khóa k_1 hoặc k_2)





Xây dựng 4: HMAC (Hash-MAC)

Được dùng rộng rãi trên Internet.

… nhưng, trước hết ta cần xem xét khái niệm hàm băm mật mã.

Tài liệu đọc thêm và trình bày

- J. Black, P. Rogaway: CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions. J. Cryptology 18(2): 111-131 (2005)
- K. Pietrzak: A Tight Bound for EMAC. ICALP (2) 2006: 168-179
- J. Black, P. Rogaway: A Block-Cipher Mode of Operation for Parallelizable Message Authentication. EUROCRYPT 2002: 384-397
- M. Bellare: New Proofs for NMAC and HMAC: Security Without Collision-Resistance. CRYPTO 2006: 602-619
- Y. Dodis, K. Pietrzak, P. Puniya: A New Mode of Operation for Block Ciphers and Length-Preserving MACs. EUROCRYPT 2008: 198-219