

## 《现代密码学》第六讲

# HASH函数和MAC (二)

# 本节主要内容

- Hash函数的定义及安全目标
- Hash函数的发展现状
- Hash函数的构造
- 消息鉴别码的定义及安全目标
- 消息鉴别码的发展现状
- 消息鉴别码的构造
- 认证加密模式

# 本节主要内容

- Hash函数的定义及安全目标
- Hash函数的发展现状
- Hash的构造
- 消息鉴别码的定义及安全目标
- 消息鉴别码的发展现状
- 消息鉴别码的构造
- 认证加密模式

# 消息鉴别码的定义及安全目标

消息认证码 (Message Authentication Code) 是定义在  $(K, M, T)$  上的算法:

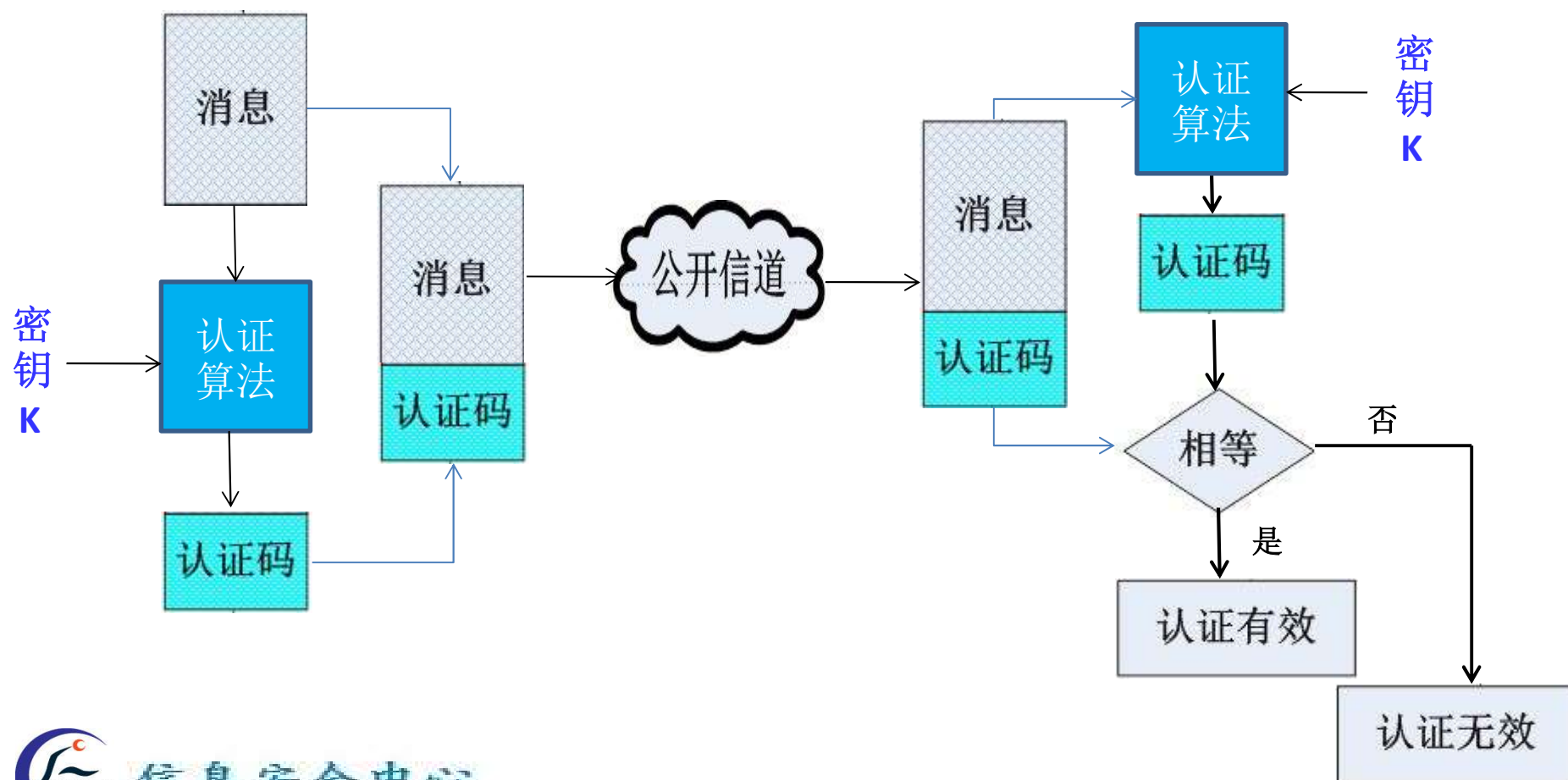
- 发送方A和接收方B共享密钥  $k \in K$ , 若A向B发送消息  $m \in M$ , 则A利用  $t = S(k, m)$  计算MAC值  $t \in T$ ;
- 接收方B对收到的  $(m^*, t^*)$ , 验证  $V(k, m^*, t^*) = \text{Accept}$  或者  $\text{Reject}$

$S$  是消息认证函数, 它利用密钥和任意长度的消息来生成一个固定长度的短数据块。若验证过程  $V(k, m^*, t^*)$  输出  $\text{Accept}$ , 接收方可以相信消息未被修改; 同时可以确信消息来自真正的发送方。

# 消息鉴别码的定义及安全目标

发送方

接收方



# 消息鉴别码的定义及安全目标

## ● 攻击者资源

### 被动攻击:

已知消息攻击: 攻击者通过窃听等手段, 获取一些消息和用同一个密钥认证这些消息所得的认证码.

### 主动攻击:

选择消息攻击: 攻击者通过选取一些消息, 发送给 oracle (MAC设备) 得到相应的认证码.

# 消息鉴别码的定义及安全目标

## ● 攻击目的

- 密钥恢复攻击：攻击者找到合法用户的的密钥 $k$ .
- 伪造攻击：攻击者在未知密钥 $k$ 的情况下，伪造一个未经过认证的 $(m, t)$ 对.

选择性伪造：如果攻击者能够对由他选择的消息 $m^*$ 进行伪造 $(m^*, t^*)$ ，那么这种伪造攻击称为选择性伪造攻击.

存在性伪造：如果攻击者只能够对一个不由他控制的消息进行伪造，那么这种伪造攻击称为存在性伪造攻击.

# 本节主要内容

- Hash函数的定义及安全目标
- Hash函数的发展现状
- Hash函数的构造
- 消息鉴别码的定义及安全目标
- 消息鉴别码的发展现状
- 消息鉴别码的构造
- 认证加密模式



# 消息鉴别码的发展现状

- M. N. Wegman and J. L. Carter. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18:143-154, 1979.
- M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22:265-279, 1981.
- Simmons, Gustavus. *Authentication theory/coding theory. Advances in Cryptology: Proceedings of CRYPTO 84. Berlin: Springer. pp. 411–431, 1985.*
- D. R. Stinson. Universal hashing and authentication codes. *Advances in Cryptology - Crypto '91*, pages 74-85, Berlin, 1991.
- 1985年，基于DES的MAC，ISO 8731-1/ ANSI X9.9
- 2002年，NIST发布标准HMAC，ANSI X9.71
- NESSIE工程推荐使用的MAC算法有TTMAC，UMAC，CBC-MAC，HMAC

# 本节主要内容

- Hash函数的定义及安全目标
- Hash函数的发展现状
- Hash函数的构造
- 消息鉴别码的定义及安全目标
- 消息鉴别码的发展现状
- 消息鉴别码的构造
- 认证加密模式

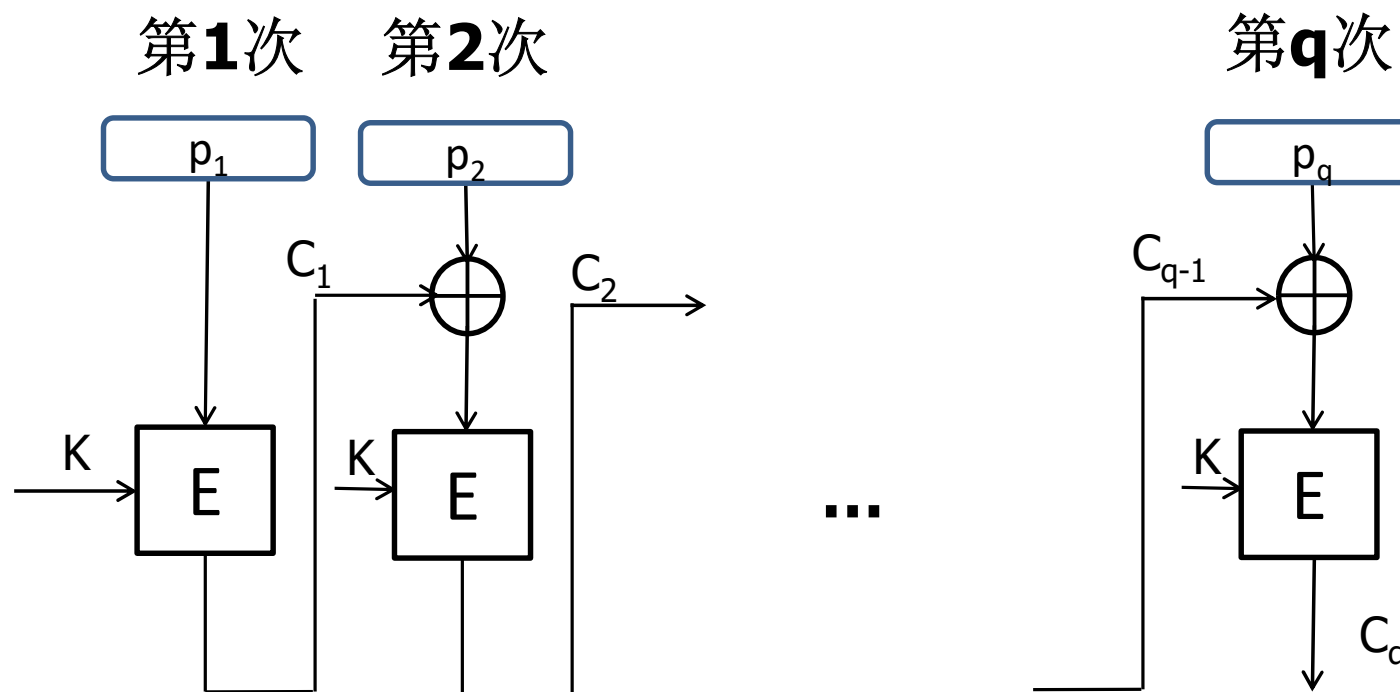
# 消息鉴别码的构造(一)

美国国家标准技术研究所 (National Institute of Standards and Technology) 于1985年5月30日发布了《计算机信息认证标准》(FIPS PUB 113 Federal Information Processing Standards Publication 113), 这个标准制定了一个基于DES数据认证算法 (Data Authentication Algorithm (DAA))。这个算法也被用在ISO 8731-1和美国国家标准局 (American National Standards Institute (ANSI)) 发布的金融机构信息认证的标准ANSI X9.9中。

# 消息鉴别码的构造(一)

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

$$P^{\leq L} = \bigcup_{i=1}^L P^i$$



# 消息鉴别码的构造(一)

若消息恰好是分组的整数倍，不考虑填充

攻击一：假定 $t_1 = E_k(D_1)$ ，则 $t_1$ 是两个分组的消息 $(D_1 || D_2)$ 的一个合法认证值，其中， $D_2 = D_1 \oplus t_1$ 。

这种攻击方法称为” cut and paste”攻击。

攻击二：攻击者想伪造消息 $D$ 的合法MAC。

首先，选择消息 $D_1$ 发送给认证者，认证者返回 $t_1 = e_k(D_1)$

然后，计算 $D_2 = D \oplus t_1$ ，把消息 $(D_1 || D_2)$ 发送给认证者，认证者返回 $t_2 = e_k(e_k(D_1) \oplus D_2)$

则 $t_2$ 是消息 $D$ 的合法认证值： $t_2 = e_k(D)$

# 消息鉴别码的构造(一)



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

## ● 基于分组密码构造举例 (CBC-MAC)

若数据不是加密算法分组长度的整数倍，则需进行消息填充，填充方法有：

- 方法1：对需要计算MAC的数据的右边填充若干个或零个“0”比特，以便得到一个比特长度是 $n$ 的整数倍的数据串。
- 方法2：对需要计算MAC的数据的右边先填充一个“1”比特，然后填充若干个或零个“0”比特，以便得到一个比特长度是 $n$ 的整数倍的数据串。
- 方法3：首先对需要计算MAC的数据的右边填充若干个或零个“0”比特，以便得到一个比特长度是 $n$ 的整数倍的数据串；其次，在所得到的数据串的左边 填充一个 $n$ 比特组，该组包含了未进行填充的数据的比特长度的二元表示，其左边用“0”补齐。



信息安全中心

# 消息鉴别码的构造(一)

课堂练习:

- 如果使用填充方法1, 上述攻击一是否还存在?
- 如果使用填充方法2, 上述攻击一是否还存在?
- 如果使用填充方法3, 上述攻击一是否还存在?



# 消息鉴别码的构造(一)

课堂练习:

- 如果使用填充方法1, 上述攻击二是否还存在?
- 如果使用填充方法2, 上述攻击二是否还存在?
- 如果使用填充方法3, 上述攻击二是否还存在?



# 消息鉴别码的构造(一)



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

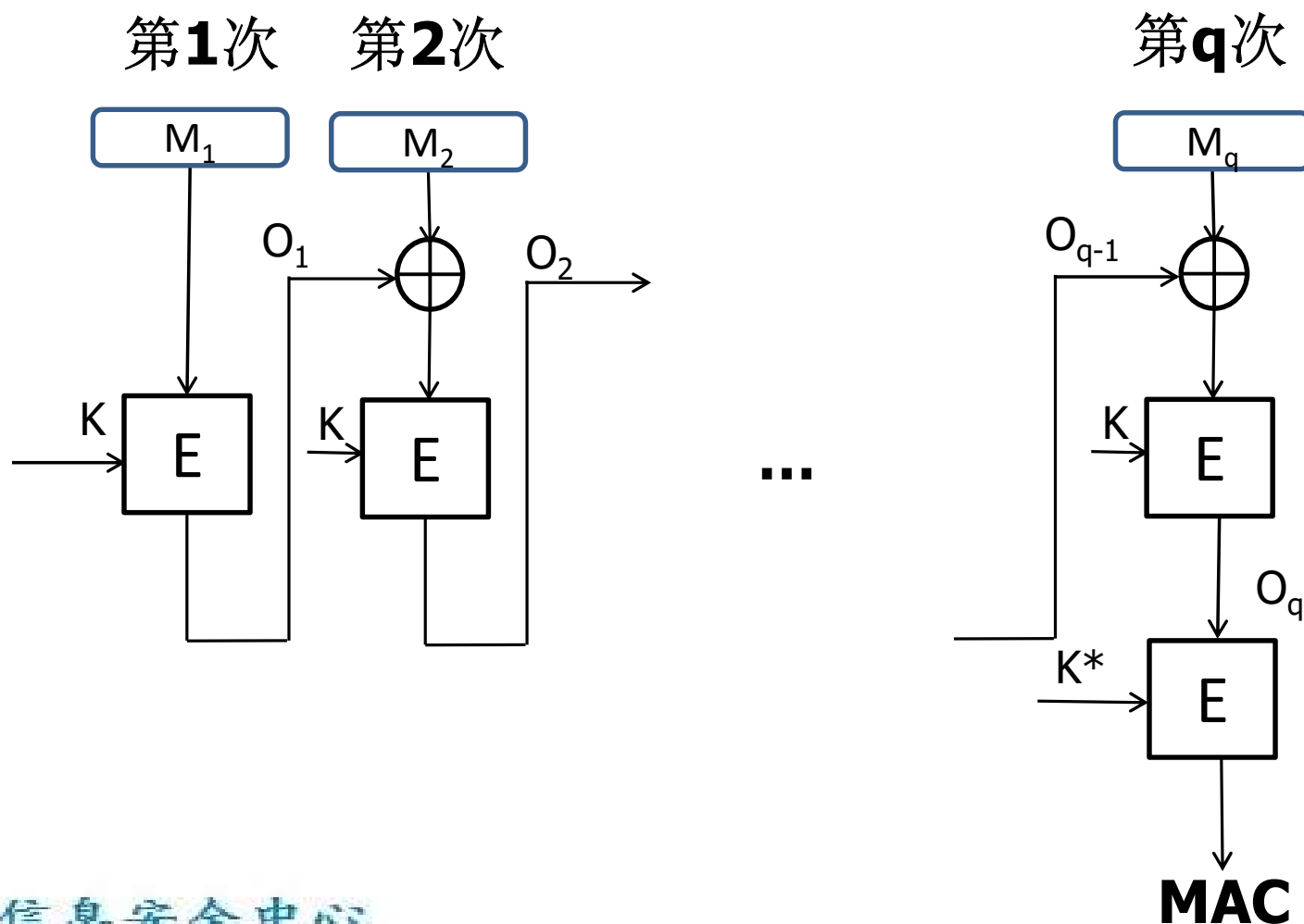
## ● 基于分组密码构造举例 (CBC-MAC)

- 填充数据，形成一串n比特数据分组 $M_1, M_2, \dots, M_q$ ;
- 使用CBC模式加密数据分组， $E_k$ 表示分组密码的加密函数，具体计算过程如下：
  1. 置 $I_0=M_1$ ，计算 $O_1=E_k(I_1)$ 。
  2. 对 $i=2, 3, \dots, q$ ，完成下列计算：
$$I_i = O_{i-1} \oplus M_i, O_i=E_k(I_i);$$
- 对 $O_q$ 进行选择处理和截断（如果 $m < n$ ），获得m比特MAC值。



# 消息鉴别码的构造(一)

## ● 基于分组密码构造举例 (ECBC-MAC)



# 消息鉴别码的构造(一)

## CBC-MAC

- 标准中规定了两种具体的选择处理方法：
  1. 选择一个密钥 $K^*$ , 计算 $MAC = E_{K^*}(O_q)$ .
  2. 选择一个密钥 $k^*$ , 计算 $MAC = E_k(D_{k^*}(O_q))$ .
- 选择处理过程可以增加密码分析者穷搜索密钥 $K$ 的难度
- 在选择处理后, 取 $n$ 比特组的最左边的 $m$ 比特构成MAC

# 消息鉴别码的构造(一)

课堂练习:

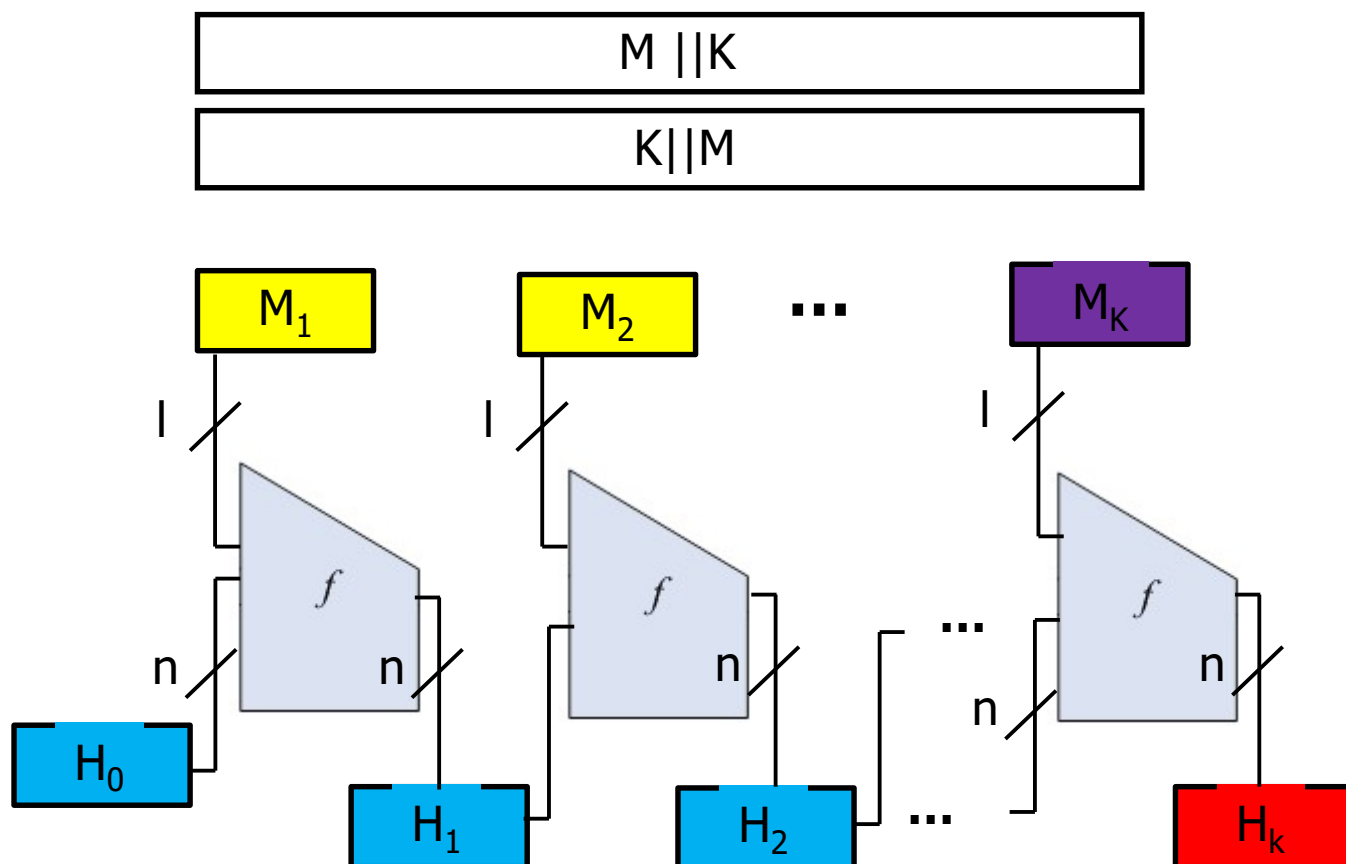
- 如果使用输出处理, 上述攻击一是否还存在?
- 如果使用输出处理, 上述攻击二是否还存在?



# 消息鉴别码的构造(二)

- HMAC是由Mihir Bellare, Ran Canetti和Hugo Krawczyk于1996年首先提出
- 2002年3月6日美国国家标准技术研究所 (National Institute of Standards and Technology) 发布了The Keyed-Hash Message Authentication Code (HMAC), 用来认证消息的起源及其完整性; 这个算法也被用在美国国家标准局 (American National Standards Institute (ANSI)) 发布的X9.71中

# 消息鉴别码的构造(二)



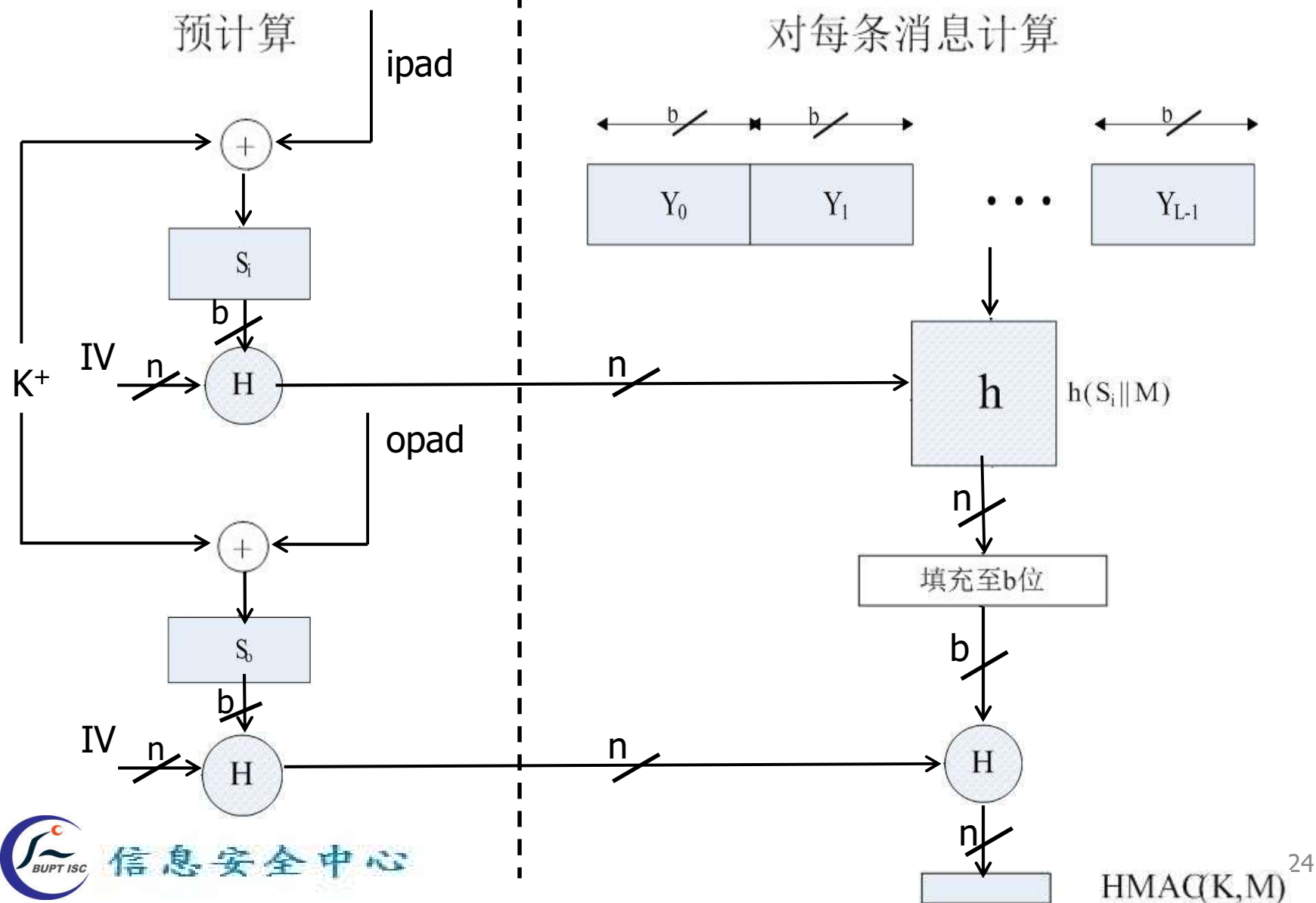
# 消息鉴别码的构造(二)

## ● HMAC计算

$$\text{MAC} = H((K \oplus \text{opad}) \parallel H(K \oplus \text{ipad} \parallel \text{text}))$$

- H是一个Hash函数
- K表示密钥
- B表示计算消息摘要时消息分块的字节长度（对SHA-256是512比特, 64字节）
- L表示消息摘要按字节计算的长度（对SHA-256是32字节）
- ipad表示0x36重复B次，opad表示0x5c重复B次。
- K可以有不超过B字节的任意长度，但一般建议K的长度不小于L。当使用长度大于B的密钥时，先用H对密钥进行杂凑，然后用得出的L字节作为HMAC的真正密钥

# 消息鉴别码的构造(二)





# 消息鉴别码的构造(二)

● 计算一个数据“文本”的HMAC的操作如下：

- 1) 在K的后面加上足够的0以得到B字节的串
- 2) 将上一步得到的B字节串与ipad异或
- 3) 将数据流“文本”接在第2步得到的B字节串后面
- 4) 将H应用于上一步的比特串
- 5) 将第1步所得到的B字节串与opad异或
- 6) 将第4步的消息摘要接在第5步的B字节串后
- 7) 应用H于上一步的比特串

# 本节主要内容

- Hash函数的定义及安全目标
- Hash函数的发展现状
- Hash函数的构造
- 消息鉴别码的定义及安全目标
- 消息鉴别码的发展现状
- 消息鉴别码的构造
- 认证加密模式

# 认证加密模式

- **Encrypt-then-MAC (EtM)**

Internet 协议安全性 (IPSec)



- **Encrypt-and-MAC (E&M)**

安全外壳协议 Secure Shell (SSH)



- **MAC-then-Encrypt (MtE)**

安全套接层协议 (SSL) 及其继任者传输层安全协议 (TLS)



2021 年 10 月 11 日, HCTR 模式正式纳入  
分组密码工作模式国家标准 GB/T 17964

# 认证加密模式

- 2000年左右，逐渐形成认证加密 (*authenticated encryption, AE*) 系统的思想
- 一个认证加密系统  $(E, D)$  定义如下：

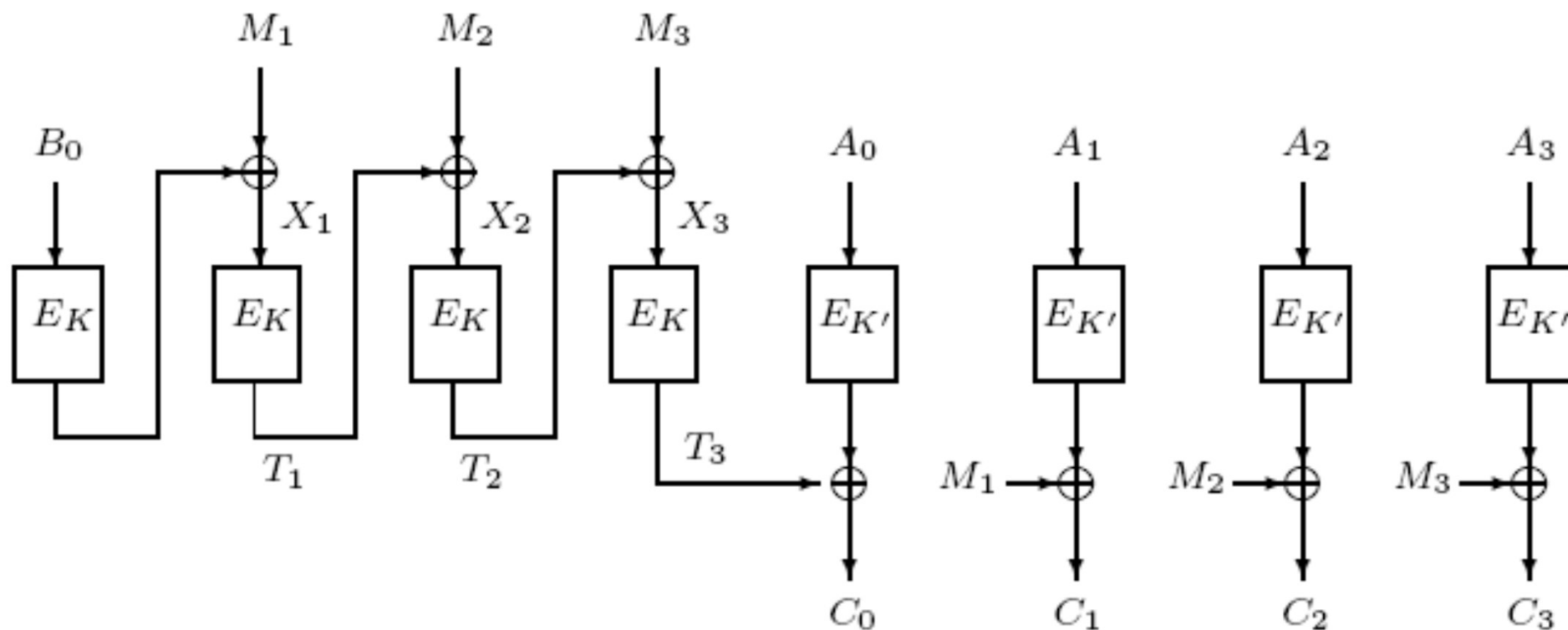
加密过程：  $E: K \times M \rightarrow C$

解密过程：  $D: K \times C \rightarrow M \cup \{\perp\}$

- 安全性：
  - CPA攻击下明文不可区分
  - 密文完整性

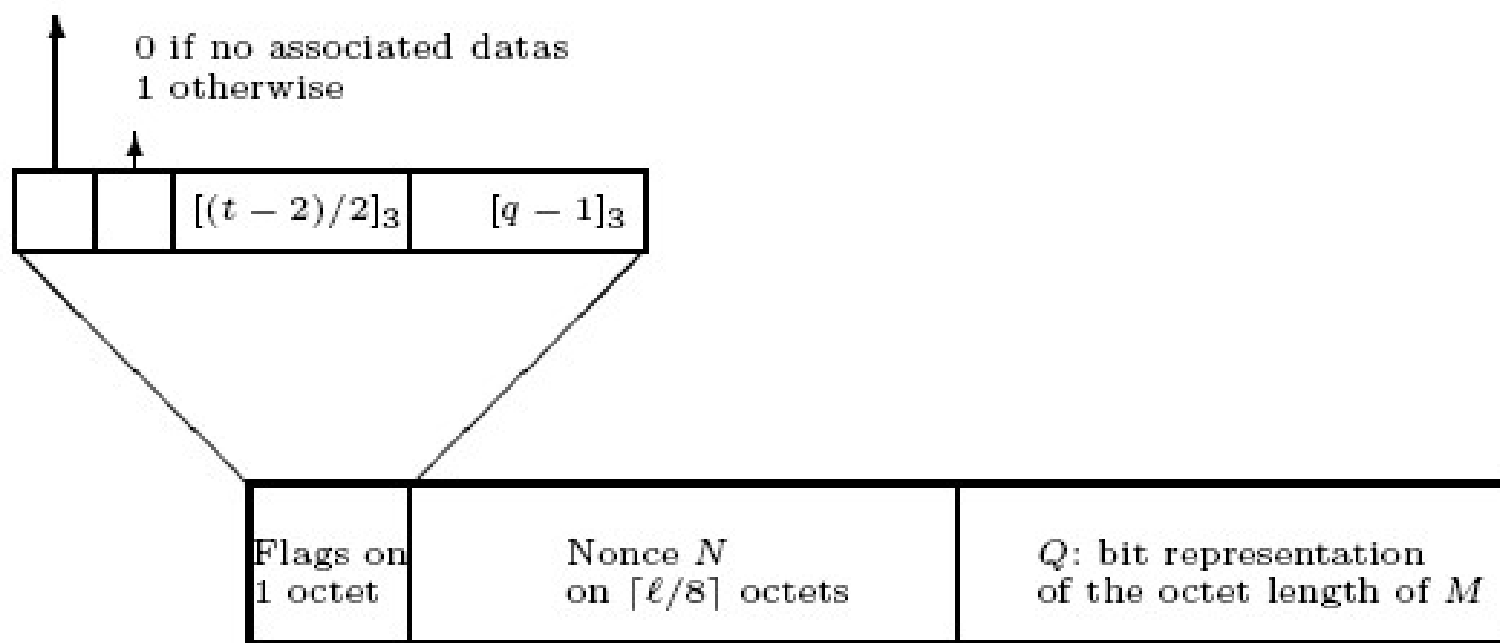
# 认证加密模式

- CCM加密认证模式



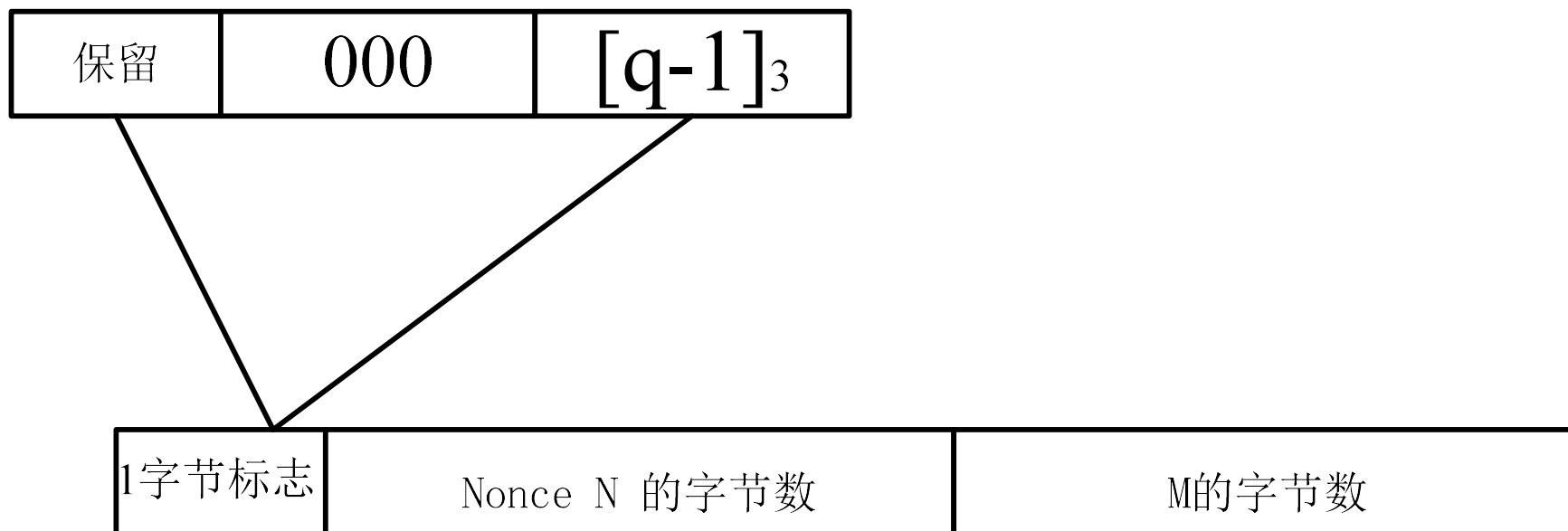
# 认证加密模式

First bit reserved for future usage



$B_0$  的设置

# 认证加密模式



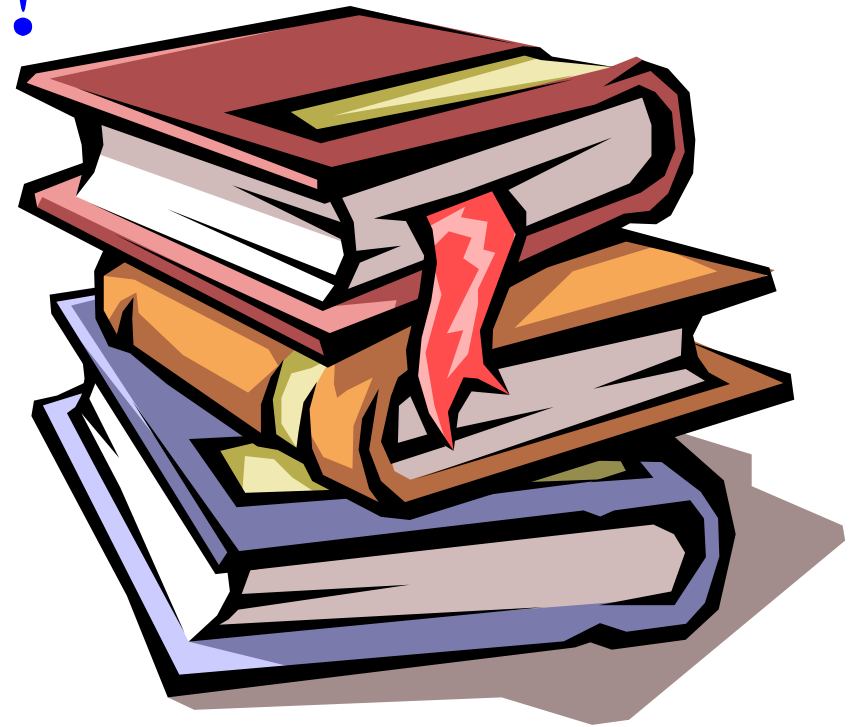
$A_0$  的设置



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

THE END !



信息安全中心