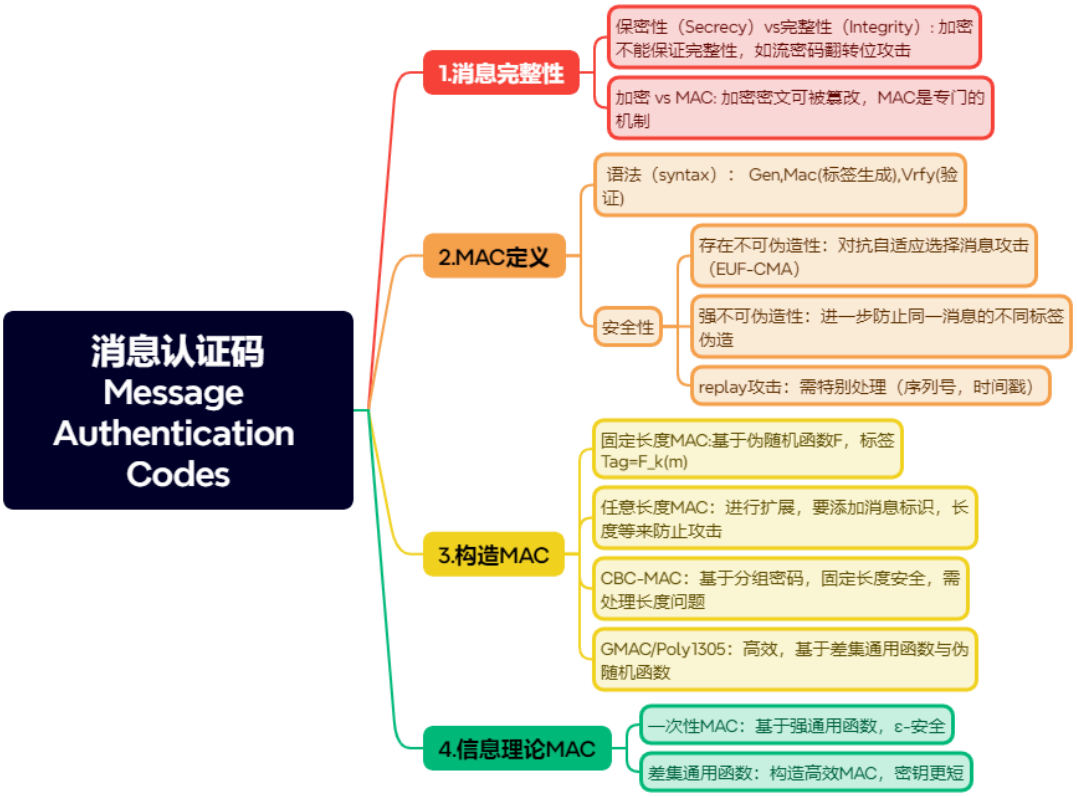
一段话总结

本章聚焦**消息认证码（MAC）**，其核心目标是保障消息完整性，防范主动攻击者的篡改与伪造。首先对比了保密性与完整性，指出加密无法提供完整性，如流密码和分组密码加密存在可被篡改的漏洞。接着定义MAC的语法，包括密钥生成、标签生成和验证算法，其安全性要求为在自适应选择消息攻击下具备**存在不可伪造性**，更强的定义是**强不可伪造性**。构造方面，基于伪随机函数可构建固定长度MAC，通过域扩展能处理任意长度消息，CBC-MAC、GMAC和Poly1305是高效实现实例。此外，还探讨了信息理论MAC，其安全性不依赖计算假设，但密钥长度受限制，且无法处理无限消息认证。

思维导图



详细总结

一、消息完整性基础

1. **保密性与完整性区别** - 保密性通过加密防止被动窃听，完整性需防范主动攻击（篡改、伪造）。
   - 加密不能提供完整性：流密码加密中翻转密文位会对应翻转明文位，如金额二进制位修改；分组密码ECB/CBC模式存在块重排、截断攻击，且任意合法长度密文可被伪造。
2. **MAC的必要性**：需独立机制检测消息篡改，确保来源真实性。

二、MAC的定义与安全性

1. 语法组成　- Gen：生成密钥k，常为均匀随机。　- Mac：概率性生成标签t=Mac_k(m)。　- Vrfy：确定性验证Vrfy_k(m,t)∈{0,1}。

2. 安全性定义　- 存在不可伪造性：在自适应选择消息攻击下，攻击者无法生成未查询消息的有效标签，概率可忽略。　- 强不可伪造性：攻击者无法生成同一消息的不同有效标签。　- Replay攻击：MAC本身不防御，需上层用序列号或时间戳处理。

三、MAC的构造方法

1. 基于伪随机函数的固定长度MAC　- 构造：Tag=F_k(m)，F为伪随机函数。　- 安全性：若F是伪随机函数，该MAC在固定长度消息下安全，伪造概率≤2^{-n}+n(n)。

2. 任意长度MAC的域扩展　- 基础思路：将长消息分块，添加消息标识、长度、索引防重排、截断、混合攻击。　- 构造4.7：添加随机标识r、长度l、索引i，Tag=<r, Mac'_k(r||l||i||m_i)>。

3. 高效实现：CBC-MAC　- 基本构造：类似CBC加密，初始向量为0^n，Tag=F_k(F_k(...F_k(0^n⊕m_1)⊕m_2)...⊕m_d)。　- 安全性：固定长度安全，处理任意长度需前缀长度或双密钥，效率为O(d)次分组加密。

4. GMAC与Poly1305　- 核心思想：基于差集通用函数h与伪随机函数F，Tag=<r, h_k(m)+F_k(r)>。　- 效率：GMAC用有限域多项式，Poly1305用素数模运算，较CBC-MAC有更好的具体安全界。

四、信息理论MAC

1. 一次性MAC　- 基于强通用函数：h_k(m)对不同m输出独立均匀，Tag=h_k(m)，伪造概率1/|T|。- 构造：h_a,b(m)=am+b mod p，p为素数，密钥(a,b)，安全界1/p。

2. 差集通用函数：h_k(m)-h_k(m')=Δ概率≤ε，构造Tag=h_k(m)+r，r均匀，安全界ε。

3. 局限性：密钥长度下限ε^{-2}，如ε=2^{-n}需密钥≥2n位，无法处理无限消息。

关键表格：不同MAC构造对比

构造方法	核心组件	消息长度	效率	安全性
固定长度 MAC	伪随机函数 F	固定 n 位	O(1)	存在不可伪造，概率 2^{-n}+negl (n)
CBC-MAC	分组密码 F	任意（需处理长度）	O(d)	固定长度安全，任意长度需改进
GMAC/Poly1305	差集通用函数 + F	任意	O (d)（更高效）	存在不可伪造，安全界 O ($(q^2+\ell)/2^n$)
信息理论 MAC	强通用函数 / 差集函数	有限	O(1)	信息理论安全，密钥长度≥ε^{-2}

关键问题

问题1：为什么加密不能保证消息完整性?

答案：加密主要解决保密性，无法防范主动攻击。例如，流密码加密中，翻转密文的某一位会导致解密后明文对应位翻转，攻击者可修改金额等关键信息；分组密码ECB模式下，密文块可被重排或截断，CBC模式中修改IV会影响首个明文块，且任意合法长度密文可被伪造，这些都表明加密本身不提供完整性保护，需独立的MAC机制。

问题2：MAC的“存在不可伪造性”和“强不可伪造性”有何区别?

答案： - 存在不可伪造性：要求攻击者无法生成任何未被查询过的消息的有效标签，即便是随机猜测，成功概率可忽略。 - 强不可伪造性：进一步要求攻击者无法生成同一消息的不同有效标签。若MAC使用规范验证（重新计算标签并比较），则存在不可伪造性可推出强不可伪造性，因为规范验证下同一消息标签唯一。

问题3：信息理论MAC与计算安全MAC的核心区别是什么?

答案： - 安全基础：信息理论MAC的安全性不依赖计算复杂性假设，基于概率理论，如强通用函数的随机性；计算安全MAC依赖伪随机函数等计算困难假设。 - 密钥限制：信息理论MAC的密钥长度受限于安全参数，如ε-安全一次性MAC需密钥长度≥ε^{-2}，无法处理无限消息认证；计算安全MAC密钥长度固定，可处理多项式数量消息。 - 效率：信息理论MAC构造简单，但密钥长；计算安全MAC如GMAC/Poly1305更高效，适合实际应用。