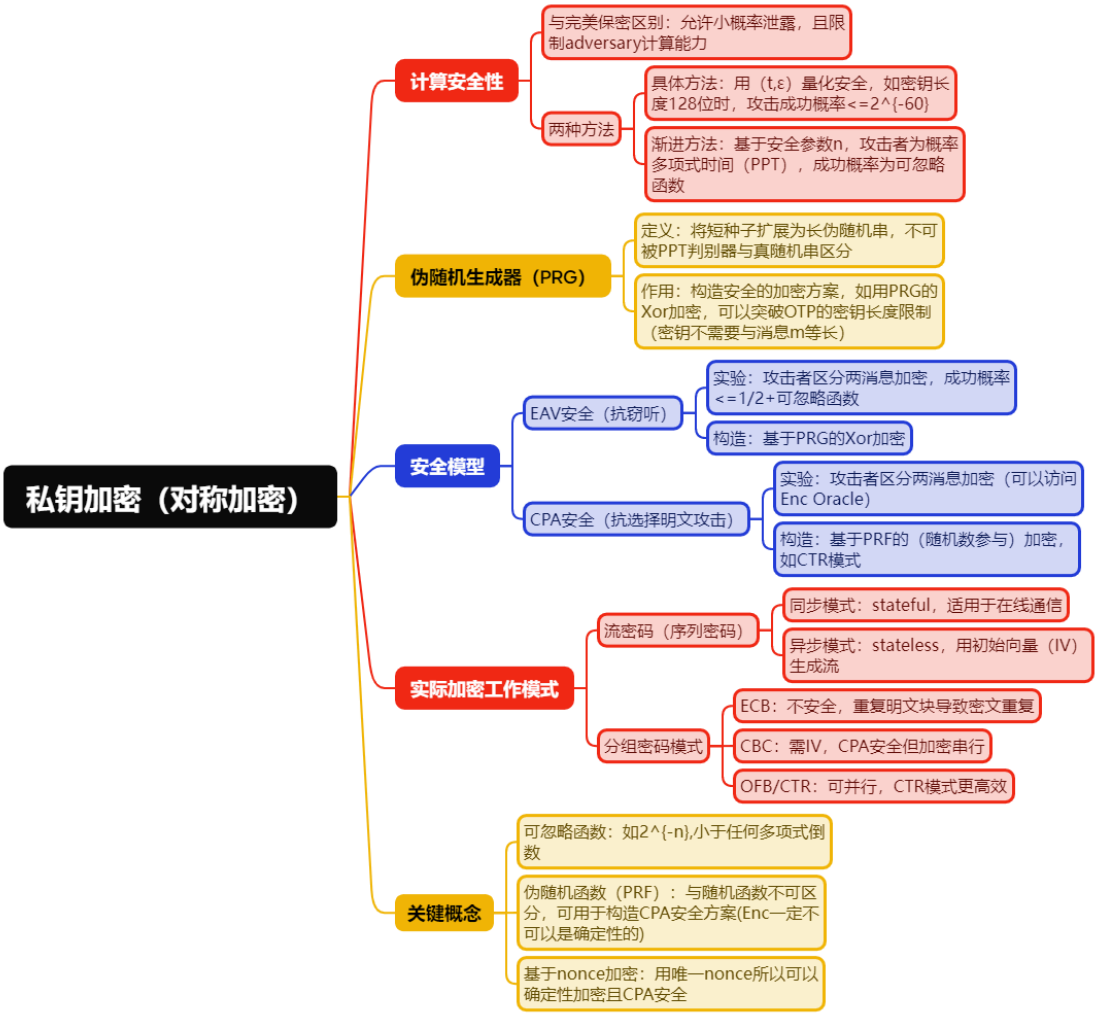
一段话总结

文档围绕私钥加密展开，介绍了**计算安全性**这一核心概念，其通过限制攻击者计算能力和允许小概率安全漏洞，突破了完美保密的局限。文中阐述了**伪随机生成器（PRG）** 和**伪随机函数（PRF）** 等关键构造，基于此定义了**EAV安全（抗窃听）** 和**CPA安全（抗选择明文攻击）** 等安全模型，并探讨了流密码、块密码的多种工作模式（如CBC、CTR）在实际加密中的应用，强调了计算安全性在理论和实践中的重要性与实现方式。

思维导图



详细总结

一、计算安全性的核心概念

1. **与完美保密的区别** - 完美保密要求无任何信息泄露，即使攻击者有无限计算能力；计算安全性仅保证对**有限计算能力**的攻击者，以**小概率**（如≤2^{-60}）泄露信息。 - 计算安全性通过**具体方法**（如(200年, 2^{-60})安全）和**渐近方法**（安全参数n，攻击者为PPT，成功概率为可忽略函数）定义。
2. **核心放松条件** - 仅对抗**高效攻击者**（PPT算法）。 - 允许**小概率失败**（如概率≤negl(n)）。

二、伪随机生成器（PRG）与伪随机函数（PRF）

1. PRG定义　- 输入n位种子，输出ℓ(n)>n位伪随机串，不可被PPT区分于真随机串。　- 例：不安全PRG如G(s)=s||(s各位异或)，因可被区分。

2. PRF定义　- 密钥函数F_k，其输出不可区分于随机函数，如F(k,x)不可被PPT通过查询区分于随机函数f(x)。 3. 作用　- PRG用于构造EAV安全加密，如将PRG输出与明文XOR，密钥n位可加密长消息。　- PRF用于构造CPA安全加密，如CTR模式中用PRF生成流。

三、安全模型与构造

1. EAV安全（抗窃听）　- 实验：攻击者输出两等长消息，接收其一的加密，成功区分概率≤1/2+negl(n)。　- 构造：基于PRG的XOR加密（如构造3.17），密钥k生成PRG(k)与明文异或。

2. CPA安全（抗选择明文攻击）　- 实验：攻击者可通过加密oracle选择明文，再区分挑战密文，成功概率≤1/2+negl(n)。　- 构造：基于PRF的随机数加密（如构造3.28），用随机r和F_k(r)异或明文，密文含r。

3. 多消息安全　- 确定性加密（如一次性密码本）无法抵抗多消息攻击，需随机化加密（如CPA安全方案）。

四、实际加密工作模式

模式	特点	安全性	应用场景
ECB	直接对每个块加密，重复明文致重复密文	不安全	禁止使用
CBC	用 IV 和前一密文块异或，串行加密	CPA 安全	需顺序处理的场景
OFB	用 PRF 生成流，异或明文，可截断	CPA 安全	需流加密，可预生成流
CTR	用 nonce + 计数器生成流，可并行	CPA 安全，高效并行	首选模式，支持并行处理
同步流密码	状态 ful，双方维护状态生成流	适用于在线通信	如 TCP 连接加密
异步流密码	用 IV 生成流，stateless	适用于无状态场景	如单次加密消息

关键问题

1. 计算安全性与完美保密的核心区别是什么？

答案：计算安全性放松了两点：①仅保证对抗有限计算能力的攻击者（PPT算法），而完美保密对抗无限计算能力；②允许安全以小概率失败（如概率≤negl(n)），而完美保密要求绝对无信息泄露。

2. 为什么CPA安全比EAV安全更强?

答案：EAV安全仅考虑被动窃听单个密文，而CPA安全允许攻击者主动选择明文加密（通过加密oracle），模拟更现实的攻击场景（如攻击者控制部分加密内容），因此安全性要求更高。

3. CTR模式相比CBC模式在实际应用中有何优势?

答案：CTR模式支持完全并行加密，因每个块的流由nonce+计数器独立生成，可同时处理多个块；而CBC模式需串行处理，前一密文块影响后一块。此外，CTR模式无需块密码可逆，且预生成流效率更高，是实际应用中的首选模式。