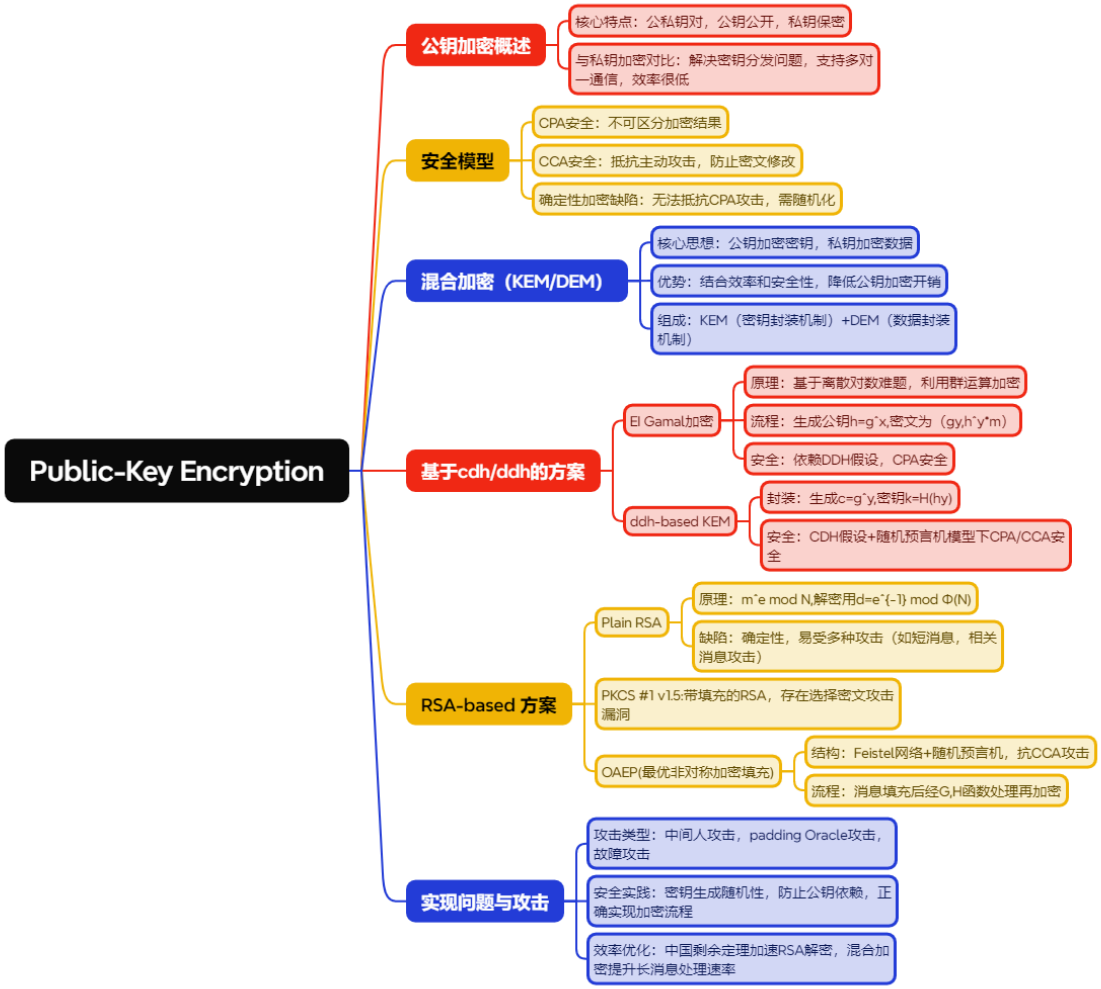
一段话总结

公钥加密通过公私钥对实现无需预共享密钥的安全通信，其核心优势在于解决密钥分发难题，适用于开放系统，但效率低于私钥加密。文档介绍了公钥加密的定义与安全模型（如CPA、CCA安全），阐述了混合加密（KEM/DEM范式）结合公钥与私钥加密优势提升效率，还详细讲解了基于Diffie–Hellman（如El Gamal）和RSA的加密方案，包括其安全性、实现方式及面临的攻击（如中间人攻击、选择密文攻击），最后强调了公钥加密在实际应用中的关键问题与注意事项。

思维导图



详细总结

一、公钥加密基础

1. 核心概念　- 公私钥对：Receiver生成(pk, sk)，pk公开用于加密，sk保密用于解密。　- 核心优势：解决私钥加密的密钥分发难题，支持开放系统中陌生方通信。　- 效率对比：公钥加密效率比私钥低2-3个数量级，私钥适用于大量数据，公钥用于密钥交换。

2. 安全模型　- CPA安全（选择明文攻击）：攻击者无法通过密文区分加密的是哪条消息，需加密算法随机化，确定性加密（如Plain RSA）不满足。　- CCA安全（选择密文攻击）：攻击者可获取任意密文的解密结果（除挑战密文），需防密文修改与伪造，如El Gamal和RSA-OAEP可实现。

二、混合加密（KEM/DEM范式）

1. 原理　- KEM（密钥封装机制）：公钥加密生成临时密钥k。　- DEM（数据封装机制）：用k私钥加密数据。

2. 效率优势　- 长消息加密时，公钥加密开销被分摊，接近私钥加密效率。　- 例：1MB消息加密，混合加密计算量约为块加密的1/16，密文长度减少50%。 3. 安全性　- CPA安全：KEM满足CPA + DEM满足EAV安全。　- CCA安全：KEM满足CCA + DEM满足CCA安全。

三、基于Diffie–Hellman的方案

1. El Gamal加密　- 流程　　- Gen：生成G, q, g，私钥x，公钥h=g^x。　　- Enc：选y，密文(c1=g^y, c2=h^y·m)。　　- Dec：m = c2 / c1^x。　- 安全：基于DDH假设，CPA安全，易受中间人攻击。

2. DDH/CDH-based KEM　- 封装：c=g^y，密钥k=H(h^y)（H为哈希函数）。　- 安全：CDH假设+随机预言机下CPA安全，gap-CDH假设下CCA安全。

四、RSA-based方案

1. Plain RSA　- 流程：Enc(m)=m^e mod N，Dec(c)=c^d mod N，d=e^(-1) mod φ(N)。　- 攻击 - 短消息攻击：m < N^(1/e)时，可直接求e次根。　　- 相关消息攻击：加密m和m+δ，通过多项式gcd破解。　　- 多接收者攻击：同一消息加密给多个公钥，利用中国剩余定理破解。

2. PKCS #1 v1.5：带固定格式填充的RSA，因填充检查可被Bleichenbacher选择密文攻击。

3. OAEP（最优非对称加密填充）　- 结构：Feistel网络+双哈希函数G、H，防CCA攻击。　- 流程：m填充后经t=m'⊕G(r)，s=r⊕H(t)，密文(s||t)^e mod N。　- 安全：RSA假设+随机预言机下CCA安全，实现需严格遵循规范，避免错误提示泄露信息。

五、实现关键问题

1. 攻击防护　- 中间人攻击：需结合数字签名验证公钥合法性。　- Padding Oracle攻击：密文解密时统一错误提示，避免泄露填充是否正确。　- 故障攻击：RSA解密时验证结果正确性，防止硬件故障导致私钥泄露。

2. 效率优化　- 中国剩余定理：RSA解密时分解为mod p和mod q计算，速度提升约4倍。　- 混合加密：长消息场景下，公钥加密仅处理密钥，数据用AES等私钥算法。

3. 密钥管理　- 避免公钥依赖：不同用户独立生成RSA modulus，防止gcd(N,N')泄露因子。　- 随机数质量：密钥生成需真随机数，避免弱随机源导致密钥碰撞。

六、方案对比表

方案	安全假设	安全级别	效率特点	应用场景
El Gamal	DDH	CPA	群运算，密文长度为 2 倍群元素	基础加密，需结合签名
Plain RSA	RSA	不安全	幂运算，密文长度 = modulus 长度	历史方案，现少用
RSA-OAEP	RSA + 随机预言机	CCA	填充 + 双哈希，抗选择密文攻击	标准 RSA 加密方案

方案	安全假设	安全级别	效率特点	应用场景
DDH-based KEM	CDH/gap-CDH	CPA/CCA	单群元素密文，需哈希函数	混合加密中的 KEM 组件

关键问题

1. 问题：为何公钥加密需要随机性，而私钥加密可以是确定性的?

答案：公钥加密中，攻击者已知公钥，若加密 deterministic，同一消息多次加密结果相同，攻击者可通过对比密文分析消息（如短消息攻击）。而私钥加密中，密钥保密，即使确定性加密，攻击者无密钥也无法破解，且私钥加密常结合IV实现随机化。

2. 问题：混合加密如何平衡效率与安全性?

答案：混合加密利用公钥加密临时密钥，私钥加密大量数据。公钥部分仅处理短密钥，开销小；私钥部分用高效算法处理数据，兼顾安全与效率。例如，1MB消息加密时，混合加密计算量约为纯公钥加密的1/16，密文长度减少约50%。

3. 问题：RSA-OAEP为何比Plain RSA更安全?

答案：Plain RSA是确定性加密，易受选择明文攻击，且无填充检查易被密文修改攻击。RSA-OAEP通过Feistel网络和双哈希函数G、H实现随机化填充，使加密结果与随机数相关，同时解密时严格验证填充格式，抵抗选择密文攻击，基于RSA假设和随机预言机模型可证明CCA安全。