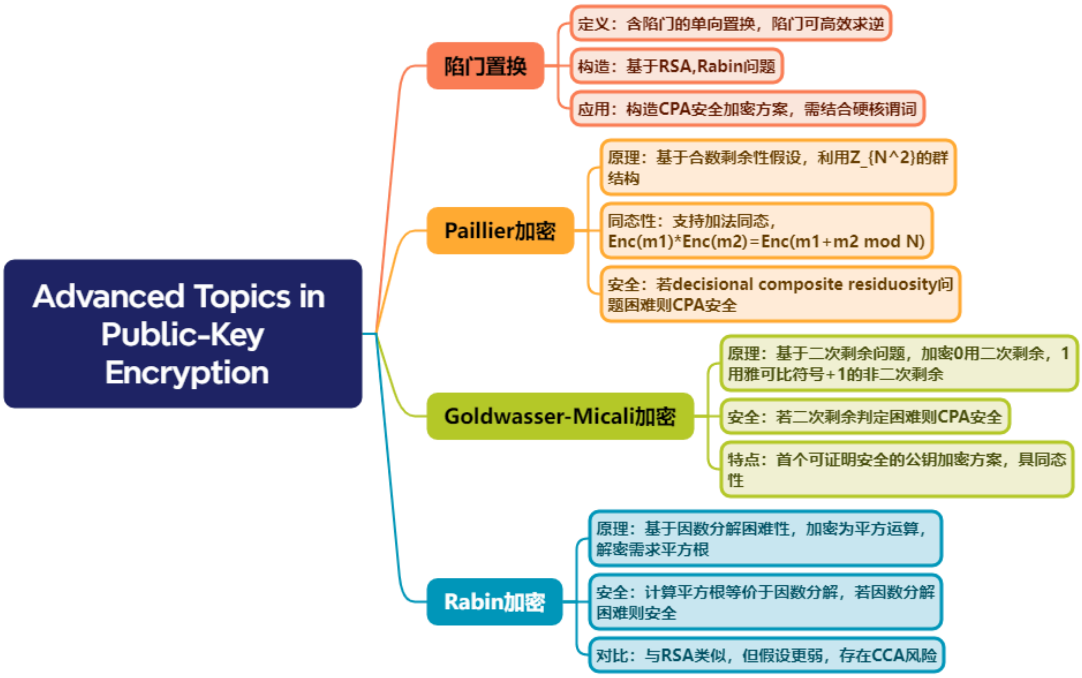
一段话总结

本章聚焦公钥加密高级主题，介绍了**陷门置换**这一单向置换的扩展概念，其能通过陷门高效求逆，可用于构造公钥加密方案；**Paillier加密**基于合数剩余性假设，具备加法同态特性，适用于安全计算等场景；**Goldwasser–Micali加密**是首个被证明CPA安全的方案，基于二次剩余问题困难性；**Rabin加密**的安全性等价于因数分解问题，与RSA类似但假设更弱。这些方案为后量子密码学提供了理论基础，展现了公钥加密在不同数学难题上的拓展与应用。

思维导图



详细总结

一、陷门置换与公钥加密

1. 陷门置换定义：　由算法(Gen, Samp, Inv)构成，Gen生成参数对(I, td)，I定义置换(f_I)，td为陷门可高效求逆，且(f_I)为单向置换。例如RSA置换(f(x)=x^e \mod N)，陷门为私钥d。

2. 基于陷门置换的加密：　利用硬核谓词（如lsb），加密时选满足硬核谓词的输入x，输出(f(x))。解密时用陷门求逆x，提取硬核谓词作为消息。

二、Paillier加密方案

1. **构造与原理**：　- 密钥生成：GenModulus生成(N=p q)，公钥N，私钥(\phi(N))。　- 加密：(Enc(m) = (1+N)^m \cdot r^N \mod N^2)，r为随机数。　- 解密：(Dec(c) = \left[\frac{c^{\phi(N)} \mod N^2 - 1}{N} \cdot \phi(N)^{-1} \mod N\right])。**同态性质**：　支持加法同态，即(Enc(m1) \cdot Enc(m2) = Enc(m1+m2 \mod N))，适用于投票统计等场景。

安全性：　**基于decisional composite residuosity假设，若无法区分均匀数与N次剩余，则CPA安全。**

三、Goldwasser–Micali加密方案

1. **基于二次剩余问题**： - 公钥：(N=p q)和(z \in QNR_N^{+1})（雅可比符号+1的非二次剩余）。 - 加密：(Enc(0)=x^2 \mod N)（x随机），(Enc(1)=z \cdot x^2 \mod N)。 - 解密：用私钥p, q判断c是否为二次剩余，输出0或1。 2. **安全性**： 若无法区分二次剩余与(QNR_N^{+1})，则CPA安全，是首个可证明安全的公钥加密方案。

四、Rabin加密方案

1. **构造与安全性**： - 加密：(Enc(m)=x^2 \mod N)，x满足lsb(x)=m。 - 解密：用私钥p, q求平方根，提取lsb。 - 安全：计算平方根等价于因数分解，若因数分解困难则安全。
2. **与RSA对比**：

方案	安全性基础	置换性质	攻击风险
Rabin	因数分解	仅在(QNR_N)上置换	存在chosen-ciphertext攻击
RSA	RSA问题	全空间置换	已知攻击不泄露私钥

五、关键技术对比

方案	数学难题	同态性	密钥长度	应用场景
Paillier	合数剩余性	加法	(2n)位	安全计算、投票
Goldwasser–Micali	二次剩余	异或	(2n)位	理论研究
Rabin	因数分解	无	(2n)位	替代RSA

关键问题

1. **问题**：Paillier加密的同态性如何实现？
答案：Paillier加密利用(\mathbb{Z}_{N^2}^*)群结构，加密时将消息m嵌入到(1+N)的指数中，乘法运算对应消息加法。具体为(Enc(m1) \cdot Enc(m2) = (1+N)^{m1}r1^N \cdot (1+N)^{m2}r2^N = (1+N)^{m1+m2}(r1r2)^N = Enc(m1+m2 \mod N))，实现加法同态。
2. **问题**：Goldwasser–Micali加密为何选择雅可比符号+1的非二次剩余？
答案**：雅可比符号+1的非二次剩余(QNR_N^{+1})与二次剩余(QR_N)在雅可比符号上均为+1，但前者无法通过平方得到。加密时，0对应(QR_N)，1对应(QNR_N^{+1})，若无法区分两者，则方案安全，利用了二次剩余判定困难性。
3. **问题**：Rabin加密与RSA的安全性假设为何不同？
答案：Rabin加密的安全性基于因数分解困难性，计算平方根等价于分解N；而RSA基于RSA问题（已知(x^e \mod N)求x），其困难性不直接等价于因数分解，可能更弱。因此Rabin的假设更基础，但存在chosen-ciphertext攻击，需额外防护。