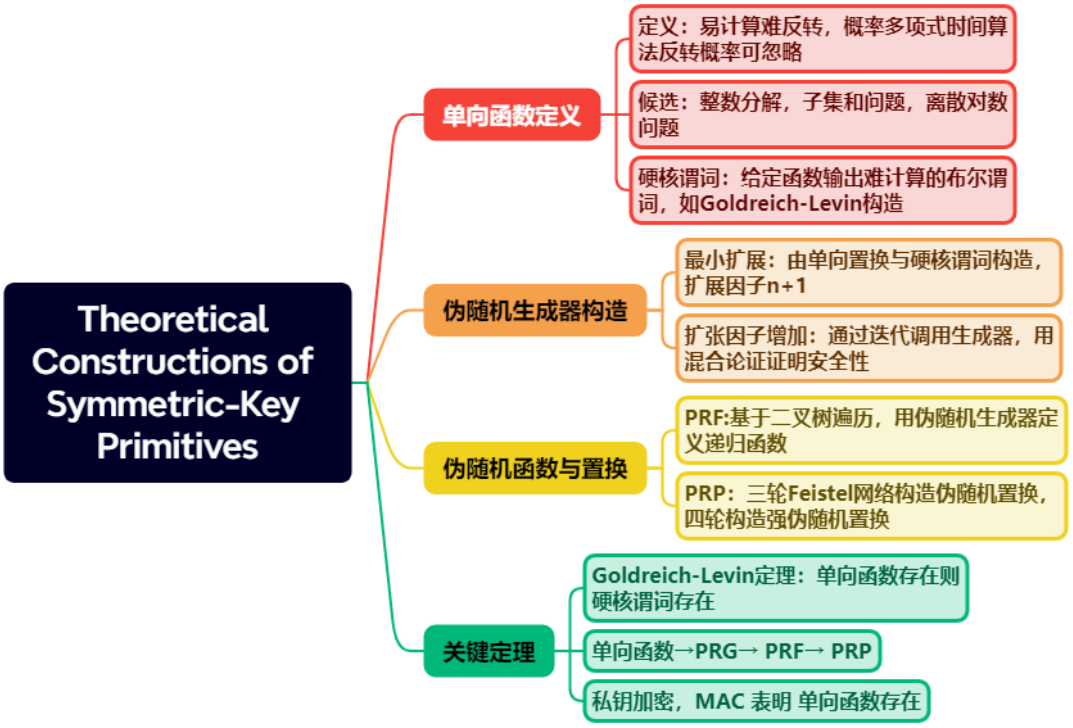
一段话总结

本章聚焦对称密钥原语的理论构造，核心在于证明**单向函数**是构建伪随机生成器、函数和置换的基础。通过定义单向函数及其硬核心谓词，利用Goldreich-Levin定理，从单向置换出发构造出最小扩展的伪随机生成器，并通过迭代扩展其扩张因子。进一步借助Feistel网络等结构，由伪随机生成器构造伪随机函数与强伪随机置换，最终证明单向函数的存在是实现非平凡私钥密码学的充要条件，揭示了理论构造与实际应用的关联及假设基础。

思维导图



详细总结

一、单向函数基础

1. 定义：函数f易计算，且对任意PPT算法A，反转概率(Pr[Invert_{A,f}(n)=1]≤negl(n))。若f是双射且长度保留，为单向置换。 _

_2. 候选函数

- *整数分解：(f*{mult}(x,y)=x·y)，限制x,y为等长素数。 - 子集和问题：(f*{ss}*(x_1,...,x_n,J)=(x_1,...,x_n,\sum*{j∈J}x_j \mod 2^n))。

- 离散对数：(f*{p,g}*(x)=g^x \mod p)，p为素数，g为生成元。 3. 硬核心谓词：对函数f，谓词hc(x)易计算，但给定f(x)时计算hc(x)概率仅略高于1/2。如Goldreich-Levin构造：(gl(x,r)=\oplus*{i=1}^n x_i·r_i)，r均匀。

二、伪随机生成器构造

1. 最小扩张（n→n+1）　- 构造：若f是单向置换，hc是硬核心谓词，定义(G(s)=f(s)||hc(s))。　- 安全性：f是置换使f(s)均匀，hc硬核心使附加位伪随机，通过区分器归约证明。

2. 任意多项式扩张　- 方法：迭代调用G，每次用前n位作为新种子，如(\hat{G}(s)=G^k(s))，k次调用得n+k位。　- 证明：混合论证，定义中间分布(H_n^j)，通过区分器归约到基生成器安全性。

三、伪随机函数与置换

1. 伪随机函数　- 构造：用2n扩张生成器G，定义(F_k(x_1...x_n)=G*{x_n}(...G*{x_1}(k)...))，如二叉树遍历。　- 安全性：归约到生成器多块不可区分性，用混合论证证明与随机函数不可区分。

2. 伪随机置换　- 三轮Feistel网络：(F^{(3)}*{k1,k2,k3}(L0,R0)=(R3,L3))，其中：　- (L1=R0, R1=L0⊕F*{k1}(R0))　- (L2=R1, R2=L1⊕F*{k2}(R1))　- (L3=R2, R3=L2⊕F*{k3}(R2))　- 强伪随机置换（四轮Feistel）：增加一轮，抵抗正反查询区分。

四、关键定理与假设

定理 / 假设	内容
单向函数存在性	是构造所有非平凡私钥原语的充要条件
Goldreich-Levin 定理	单向函数存在→存在硬核心谓词
构造链	单向函数→伪随机生成器→函数→置换
必要性证明	EAV 安全加密（消息长 2 倍于密钥）→单向函数

五、计算不可区分性

1. 定义：两概率 ensemble (X,Y)，对任意PPT区分器D，(|Pr[D(X_n)=1]-Pr[D(Y_n)=1]|≤negl(n))。

2. 应用：伪随机生成器定义为(G(U_n) \stackrel{c}{≡} U_{ℓ(n)})，多样本不可区分性定理支持多块扩展。

关键问题

1. 单向函数在对称密钥构造中的核心作用是什么?

答案：单向函数是对称密钥原语的理论基础，其存在是构造伪随机生成器、函数和置换的充要条件。通过硬核心谓词，单向函数的"难反转性"转化为伪随机序列的"不可预测性"，进而构建各类密码学原语，确保从理论上奠定安全性基础。

2. 如何从单向函数逐步构造出伪随机置换?

答案：首先由单向置换与硬核心谓词构造扩张因子n+1的伪随机生成器，再通过迭代扩展其扩张因子。接着用生成器构建基于二叉树遍历的伪随机函数，最后利用三轮或四轮Feistel网络，将伪随机函数转化为伪随机置换，通过多轮函数迭代和结构设计确保置换的伪随机性和可逆性。

3. 为什么说单向函数是私钥密码学的最小假设?

答案：一方面，单向函数可构造所有非平凡私钥原语（如加密、MAC）；另一方面，非平凡私钥加密（消息长于密钥）或安全MAC必然蕴含单向函数存在。这形成充要关系，表明单向函数是私钥密码学不可再弱的假设，无法在更弱假设下实现同等安全构造。