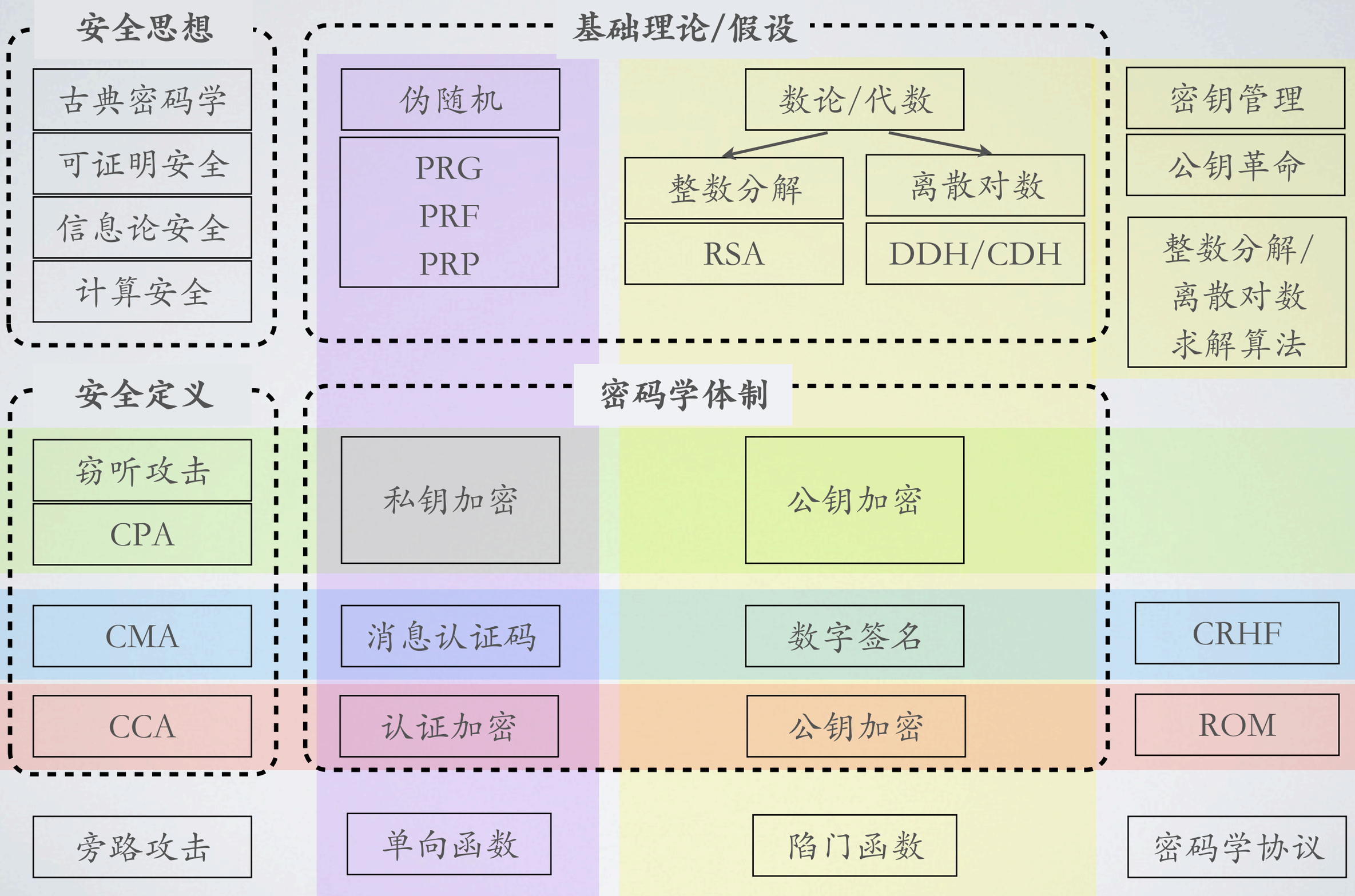
安全思想
古典密码学
可证明安全
信息论安全
计算安全
基础理论/假设
伪随机
PRG
PRF
PRP
数论/代数
整数分解
离散对数
RSA
DDH/CDH
密钥管理
公钥革命
整数分解/
离散对数
求解算法
安全定义
窃听攻击
CPA
CMA
CCA
旁路攻击
密码学体制
私钥加密
公钥加密
消息认证码
数字签名
认证加密
公钥加密
单向函数
陷门函数
CRHF
ROM
密码学协议