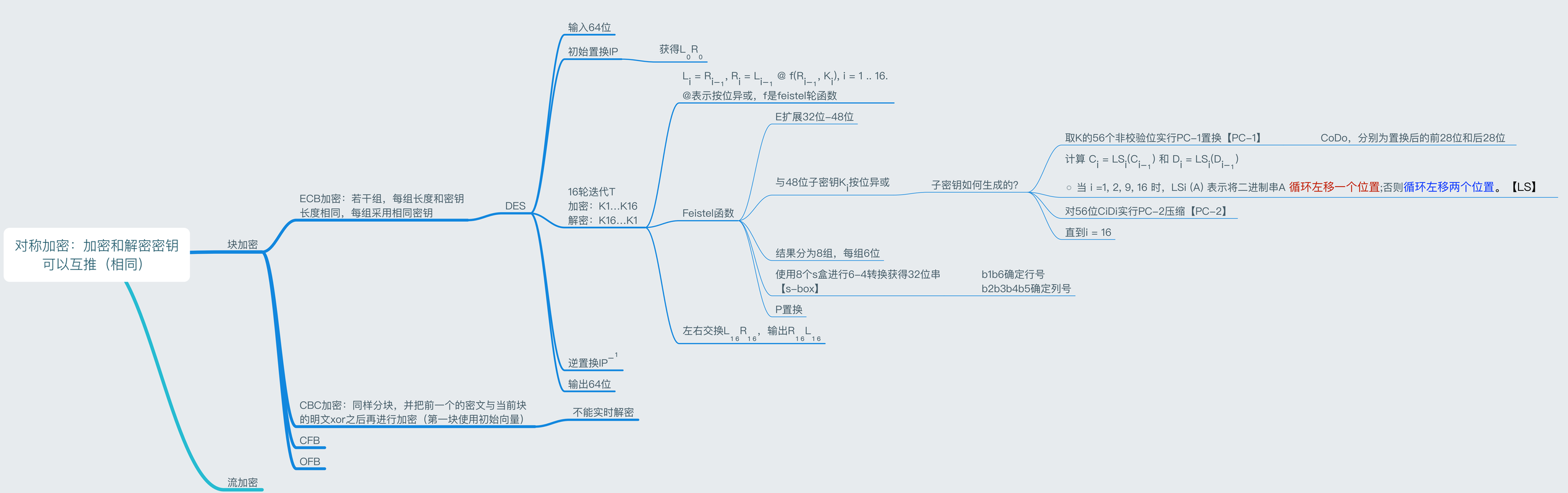
对称加密：加密和解密密钥可以互推（相同）
块加密
流加密
ECB加密：若干组，每组长度和密钥长度相同，每组采用相同密钥
DES
输入64位
初始置换IP
获得L0 R0
Li = Ri−1, Ri = Li−1 @ f(Ri−1, Ki), i = 1 .. 16.
@表示按位异或，f是feistel轮函数
16轮迭代T
加密：K1...K16
解密：K16...K1
Feistel函数
E扩展32位–48位
与48位子密钥Ki按位异或
子密钥如何生成的?
取K的56个非校验位实行PC–1置换【PC–1】
CoDo，分别为置换后的前28位和后28位
计算 Ci = LSi(Ci−1) 和 Di = LSi(Di−1)
○ 当 i =1, 2, 9, 16 时，LSi (A) 表示将二进制串A 循环左移一个位置;否则循环左移两个位置。【LS】
对56位CiDi实行PC–2压缩【PC–2】
直到i = 16
结果分为8组，每组6位
使用8个s盒进行6–4转换获得32位串
【s–box】
b1b6确定行号
b2b3b4b5确定列号
P置换
左右交换L16 R16，输出R16 L16
逆置换IP−1
输出64位
CBC加密：同样分块，并把前一个的密文与当前块的明文xor之后再进行加密（第一块使用初始向量）
不能实时解密
CFB
OFB