自由主题

密钥扩展

- 初始密钥处理
  - 密钥拆分 — 将128bit密钥拆分为4个32bit数据
  - 密钥异或
    - K0与FK0异或得到k0
    - K1与FK1异或得到k1
    - K2与FK2异或得到k2
    - K3与FK3异或得到k3
- 轮密钥生成流程
  - 循环轮次定义 — 共进行32轮密钥拓展
  - 每轮密钥生成步骤
    - 生成sbox_input — 使用ki+1,ki+2,ki+3与CKi异或
    - 执行盒变换
      - sbox_input拆分为4个8bit数据
      - 分别对4个8bit数据进行盒变换
      - 合并盒变换输出为sbox_output
    - 生成移位结果
      - y13: sbox_output左移13位
      - y23: sbox_output左移23位
    - 计算rki — rki=sbox_output⊕y13⊕y23⊕ki
- 固定参数说明
  - FK0,FK1,FK2,FK3定义
  - CK0至CK31定义