章节安排

Outline

SM4侧信道攻击实验

实 验 目 的

- **实验3 ： SM4侧信道攻击实验（4学时）**

  实验目的：掌握SM4算法的实现过程，SM4算法软件实现方法，采用CPA攻击方法进行侧信道分析

实 验 内 容

- **实验3：SM4侧信道攻击实验（4学时）**
- **实验要求：**
- 1 SM4算法实现
- 补充SM4算法代码，并与开发板进行通信，验证开发板写入的SM4软件实现算法是否正确。
- 2 SM4软件实现数据采集，程序下载到开发板
- 将已完成的SM4软件实现下载烧写到开发板，采集SM4软件实现能量轨迹数据。
- 3 SM4侧信道攻击
- 使用采集到的轨迹数据，掌握SM4软件实现的CPA攻击方法，实现侧信道攻击。