章节安排

Outline

AES侧信道攻击实验

实 验 目 的

- **实验1：AES侧信道攻击实验（4学时）**

  实验目的：掌握AES算法的加解密程序实现方法，了解侧信道攻击的基本步骤

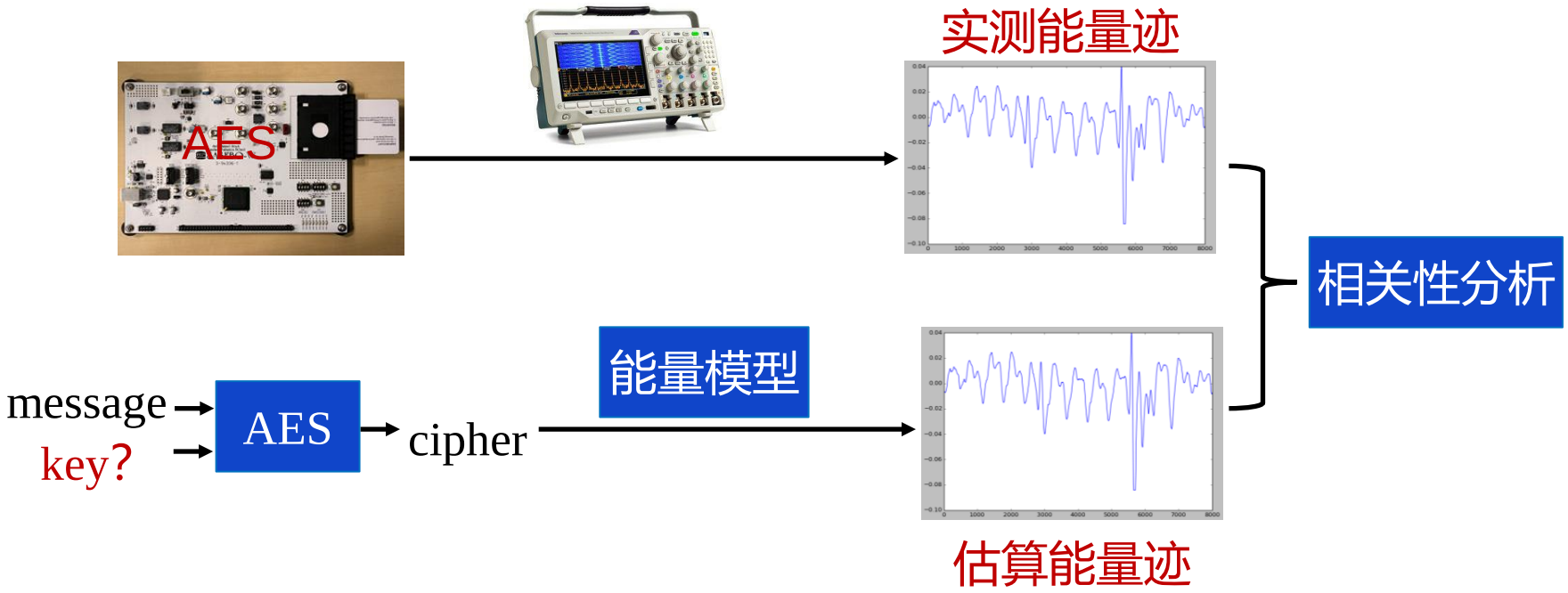
  掌握对AES软件实现的CPA攻击方法

实 验 内 容

- **实验1：AES侧信道攻击实验（4学时）**
- **实验要求：**
- 1 AES算法实现
- 掌握AES算法的加解密流程、特性和程序实现方法。基于实验环境，补全AES软件程序。
- 2 AES加密轨迹采集
- 下载已完成的AES程序到开发板并调试，通过示波器，完成加密轨迹数据采集。
- 3 AES侧信道攻击
- 了解侧信道攻击的基本步骤，使用采集到的加密轨迹数据，实现侧信道CPA攻击。

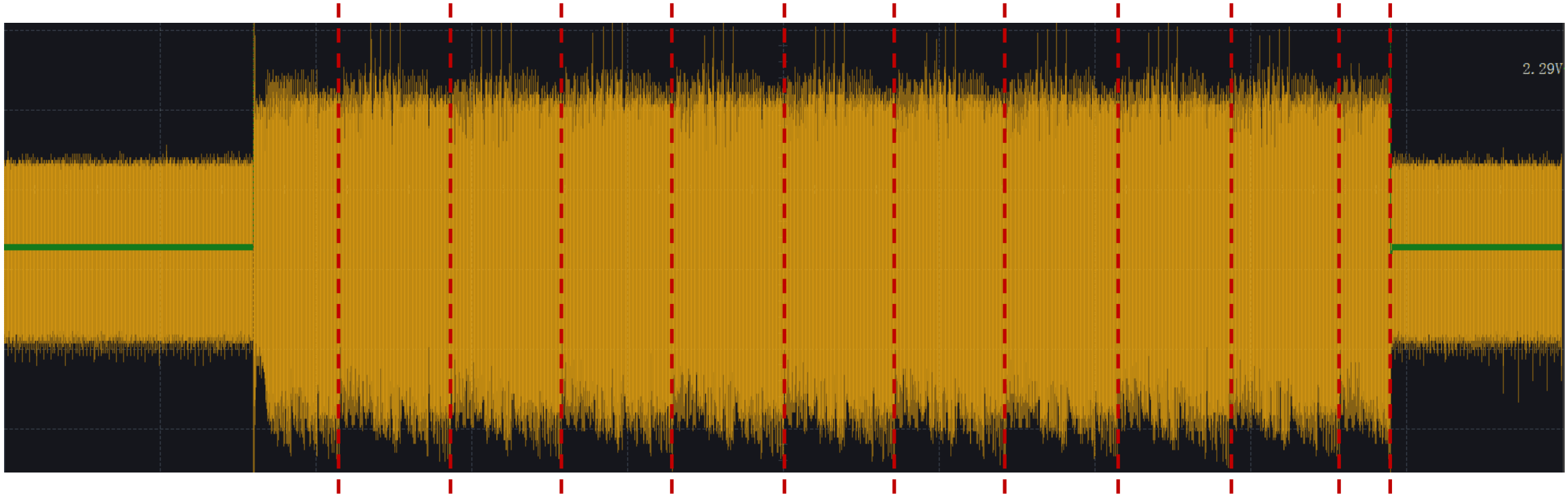
实 验 原 理

- AES能量侧信道攻击
  - 能量迹的采集
  - 理论能量迹的估算
  - 相关性分析
  - 密钥恢复



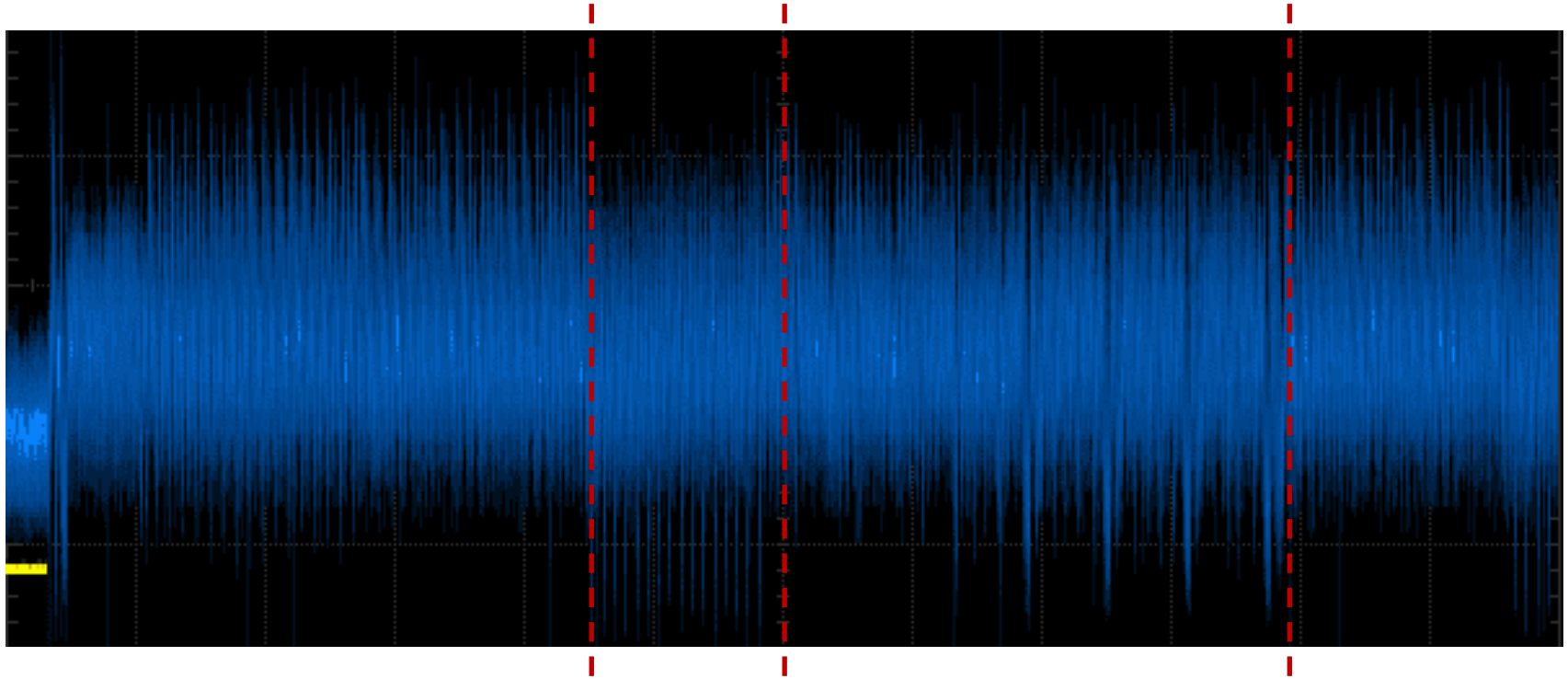
实 验 原 理

- AES能量侧信道攻击
  - 能量迹的采集



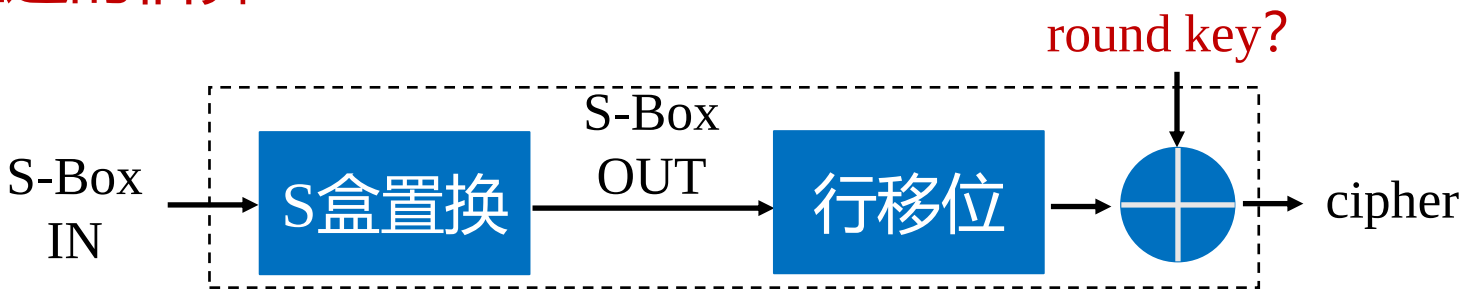
实 验 原 理

- AES能量侧信道攻击
  - 能量迹的采集



实 验 原 理

- AES能量侧信道攻击(最后一轮为例)
  - 理论能量迹的估算



$$C = \begin{bmatrix} c_{11} & \cdots & c_{1k} \\ \vdots & \ddots & \vdots \\ c_{N1} & \cdots & c_{Nk} \end{bmatrix}$$

密文

$$SO = \begin{bmatrix} so_{1,0} & \cdots & so_{1,255} \\ \vdots & \ddots & \vdots \\ so_{N,0} & \cdots & so_{N,255} \end{bmatrix}$$

S-Box OUT

$$SI = \begin{bmatrix} si_{1,0} & \cdots & si_{1,255} \\ \vdots & \ddots & \vdots \\ si_{N,0} & \cdots & si_{N,255} \end{bmatrix}$$

S-Box IN

实 验 原 理

- 攻击步骤（以攻击第一轮为例）
  - S1: 加密N（约10000）条明文并用示波器采集能量迹（Power trace）
  - S2: 对这N条明文，对于每个密钥字节的可能取值key[i] ∈ [0，255]，1 ≤ i ≤ 16，分别计算得到N个S-Box IN和S-Box OUT的值

$$T = \begin{bmatrix} t_{11} & \cdots & t_{1k} \\ \vdots & \ddots & \vdots \\ t_{N1} & \cdots & t_{Nk} \end{bmatrix}$$

能量迹

$$SI = \begin{bmatrix} si_{1,0} & \cdots & si_{1,255} \\ \vdots & \ddots & \vdots \\ si_{N,0} & \cdots & si_{N,255} \end{bmatrix}$$

S-Box IN

$$SO = \begin{bmatrix} so_{1,0} & \cdots & so_{1,255} \\ \vdots & \ddots & \vdots \\ so_{N,0} & \cdots & so_{N,255} \end{bmatrix}$$

S-Box OUT

实 验 原 理

- AES能量侧信道攻击
  - 相关性分析
  - 密钥恢复