|  |  |  |  |
| --- | --- | --- | --- |
| 泄露分析报告 | | | 20230802143645196543 |
| 报告类型： | ☑仿真芯片数据 ☐实时芯片数据 | 报告完成时间:2023年8月2日 | |
| 芯片ip端口： | 127.0.0.1:8000 |
| 侧信道分析方法 | 结论 | | |
| DPA(差分功耗分析) | 分析原理：使用统计方法分析测量集，以识别数据的相关性 分析结果：LSB=1时AES S-box输出见曲线（上），LSB=0时AES S-box输出见曲线（下） | | |
| TA(模板分析) | 未检测 | | |
| CPA(相关性功耗分析) | 分析原理：使用统计方法分析测量集，以识别数据的相关性 分析结果(汉明权重)：0b11101000，0b1001111, 0b10011010 | | |
| SPA(简单功耗分析) | 未检测 | | |