

抗差分功耗分析攻击的 AES S 盒电路设计

曾永红, 叶旭鸣

(航天科工集团三院八三五七研究所, 天津 300141)

摘要: 提出一种抗差分功耗分析攻击的高级加密标准(AES)异步 S 盒电路。采用复合域算法实现精简的 S 盒结构, 通过引入单轨异步流水线降低整个 S 盒的功耗, 在单轨电路中局部采用异步双轨电路, 利用随机数控制下的数据扰乱机制, 改善电路的抗差分功耗分析攻击性能, 建立 S 盒差分功耗分析攻击仿真平台, 对设计的相关性能进行了仿真验证和测试。

关键词: 差分功耗分析; 高级加密标准; S 盒; 数据扰乱机制

Design of AES S-box Circuit with Anti-DPA Attack

ZENG Yong-hong, YE Xu-ming

(Institute 8357, Third Academy of China Aerospace Science and Industry Corporation, Tianjin 300141)

【Abstract】 This paper proposes an asynchronous Advanced Encryption Standard(AES) S-box circuit with the performance of anti-Differential Power Analysis(DPA) attacks. In this S-box, composite-field arithmetic is used to attain the compact S-box architecture, the single-rail asynchronous pipelines are inserted in the data-path circuits to reduce the S-box circuit's power, its property of anti-DPA attack is improved by introducing the locally inserting asynchronous dual-rail circuits and the disordered-data mechanism. Simulating validation and test are done by the presented simulating DPA attack platforms for the S-box.

【Key words】 Differential Power Analysis(DPA); Advanced Encryption Standard(AES); S-box; disordered-data mechanism

1 概述

2001 年, 高级加密标准(Advanced Encryption Standard, AES)正式发布并投入使用, 但随着技术的进步, 多种攻击方法对 AES 的密钥安全造成了越来越大的压力。文献[1]提出一种差分功耗分析(Differential Power Analysis, DPA)攻击方法, 对 AES 构成了巨大的威胁, 实践证明没有采取任何保护措施 AES 电路是可被 DPA 攻击成功的。S 盒是 AES 电路中唯一的非线性转换结构, S 盒的数量和实现方式决定了 AES 协处理器诸如尺寸、速度和功耗方面的性能, S 盒常会成为攻击者对 AES 电路实施 DPA 攻击的重点部位, 提高 S 盒的抗 DPA 能力对 AES 的安全性具有重要意义^[2]。如何提高电路的抗 DPA 攻击性能是一项需要反复权衡的工作, 伴随系统的抗 DPA 攻击性能的提高, 电路会在速度、功耗或面积等指标性能上有所降低。如何减少这些负面影响, 在防范措施设计过程中是不能忽略的。本文设计了一种以合理功耗和面积为代价的抗 DPA 攻击的 AES S 盒电路实现方案。

2 S 盒的基本实现架构

本文讨论针对面积和功耗都有要求的嵌入式系统使用的精简 S 盒结构, 原理上采用的是基于 $GF(2^8)$ 复合域求逆运算的加密和解密操作共用部分 S 盒电路的方案^[3]。在该算法实现中将有限域 $GF(2^8)$ 求逆运算, 转换成 $GF((2^n)^m)$ 下的求逆; 这里 $n \times m = 8$, $GF((2^n)^m)$ 与 $GF(2^8)$ 是同构的。而在众多的复合域 S 盒实现架构中, 笔者基本遵循文献[4]提出的基于 $GF(((2^2)^2)^2)$ 的 S 盒架构(简称 Satoh S 盒), 在文献[5]中给出 $GF(((2^2)^2)^2)$ 的 S 盒电路详细的数学推导和电路实现。同时, 为实现 S 盒的低功耗, 在 Satoh S 盒的基础上, 通过在 S 盒中加入异步流水线实现一个单轨异步 S 盒, 该电路大体上可以分为数据通道和握手通道 2 个部分。数据通道的电路结构

如图 1 所示。

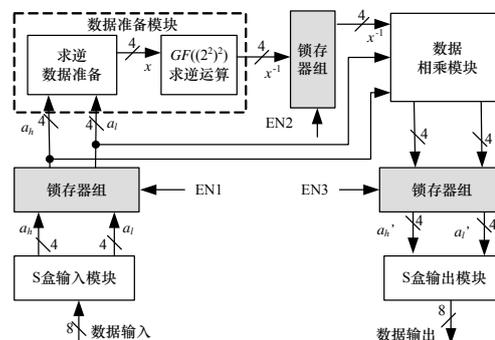


图 1 异步 S 盒数据通道框图

在完成数据通道的模块划分后, 在各个模块之间插入电平锁存器组构成异步流水线的数据处理模块, 其各锁存器组由异步握手通道产生的使能信号来控制; 异步 S 盒各个模块的详细设计实现参考文献[3]。

3 S 盒的抗 DPA 攻击策略

整个异步 S 盒电路的功耗大体由握手电路功耗、组合逻辑电路功耗、锁存电路功耗和噪声功耗组成。其中, 为常量的握手电路功耗和随机变化的噪声功耗与数据无关, 而另外 2 种功耗则与数据相关, 能够被攻击者利用来实施对 S 盒的 DPA 攻击。本文的 S 盒抗 DPA 攻击优化设计主要基于 2 点策略: (1) 通过减小上述电路泄漏的功耗信息, 使其信噪比

基金项目: 航天支撑技术基金资助项目(618101040702)

作者简介: 曾永红(1974—), 男, 博士, 主研方向: 片上系统, 可编程片上系统; 叶旭鸣, 高级工程师

收稿日期: 2009-10-10 **E-mail:** zyher1974@163.com

降低到无法满足 DPA 观测的要求；(2)采用已被证明对 DPA 攻击具有十分强的鲁棒性的随机数控制的逻辑电路^[6]。

对于双轨异步电路任何有效的正/负逻辑，在电路实现上都是由正相和互补逻辑实现电路构成，且其操作机制也决定了任何数据处理过程的电流消耗是平衡的，因此，它具有很好的抗 DPA 攻击性能^[7]。通过在单轨异步 S 盒中部分引入双轨逻辑，使数据包异步电路泄漏的与数据有关的功耗信息减小到无法被 DPA 攻击的程度，同时考虑到采用双轨逻辑的模块功耗其实已经远高于 S 盒中采用单轨编码的模块。这时 S 盒所泄漏的被 DPA 攻击利用的信息其实已被降低到十分可观的程度。另外，由于双轨电路是一种完全的数据流驱动的电，与同步电路相比，攻击者很难确定异步电路的时钟周期，进而难以确定攻击用相关曲线的起始点，在一定程度上提高了 S 盒的抗 DPA 攻击性能。其次，考虑到双轨逻辑电路由正相和互补逻辑电路构成。在保证电路的逻辑功能正确下，采用随机数选择，使电路在正向逻辑和反向逻辑间进行随机切换。鉴于正相和互补逻辑电路的功耗与数据的相关性是不一致的，进而会影响最终电路实现的输入数据与功耗之间的相关性。

4 电路实现

局部采用双轨逻辑异步 S 盒的数据通道结构框图如图 2 所示。

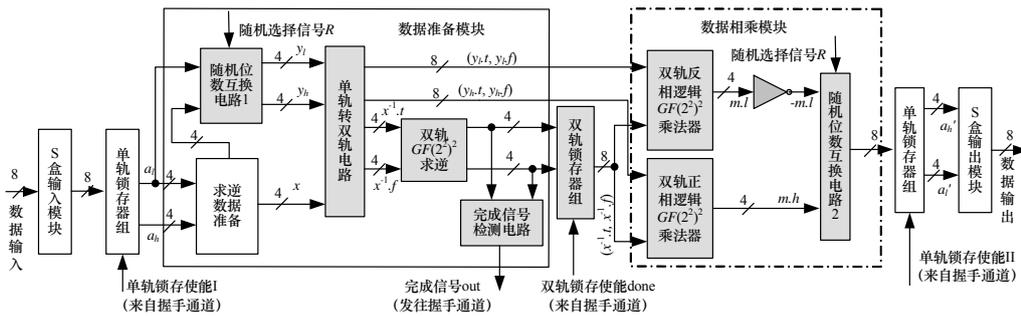


图 2 S 盒电路的数据通道结构框图

在求逆运算和数据相乘模块中引入双轨逻辑。双轨逻辑在完成有效数据运算操作后，正相逻辑和反相逻辑电路的输出值是互补的；而在双轨逻辑处于“空闲”状态时，它们的输出都为 0。结合 S 盒的结构特点，在数据相乘模块中只采用一个双轨乘法器。另外，为保证双轨反相逻辑电路的有效数据输出的正确性，要将反相逻辑电路的 4 位输出反相： $m_l \rightarrow \bar{m}_l$ 。此外，数据通道中还要增加单轨转双轨电路、双轨锁存器组和完成信号检测电路。

另外，数据通道利用 2 个随机位数互换电路扰乱 S 盒电路数据与泄漏的功耗信息之间的相关性，称为“数据扰乱”机制。数据扰乱下的求逆运算过程如图 3 所示。

主要利用随机选择信号 R 来控制输入信号 In_0 和 In_1 互换，当 $R=0$ 时， $In_0 \rightarrow Out_0$ ， $In_1 \rightarrow Out_1$ ；当 $R=1$ 时，输入通道互换 ($In_0 \rightarrow Out_1$ ， $In_1 \rightarrow Out_0$)。由于从数据 $\{a_h, a_l\}$ 到 $\{x^1.t, x^1.f\}$ 的过程和数据扰乱机制无关，在图 3 中被省略(用虚线代替)。数据扰乱的关键是 2 个由同一随机数 R 控制的位数转换电路。结合图 2 所示的 S 盒结构，数据扰乱机制下的求逆流程如下：当 $R=1$ 时，位数互换电路 1 使 $y_h=a_l$ ， $y_l=a_h$ ；经过数据相乘模块后求得的高 4 位 m_h (或低 4 位 m_l)，数据其实是正常状态下的低 4 位 a_l' (或互补的高 4 位 a_h') 数据。将数据 m_l 反

相后，通过相同的随机数输入 R 控制下的位数互换电路 2 得到正确的求逆运算数据输出 $\{a_h', a_l'\}$ 。由于数据 R 是随机的，加之双轨乘法器中的正相和反相逻辑乘法器的功耗存在差异。因此，对于同样的数据输入 $\{a_h, a_l\} \rightarrow \{a_h', a_l'\}$ 的求逆运算，其功耗频谱是不一样的，这样就达到扰乱数据输入与泄漏功耗信息间的相关性目的。

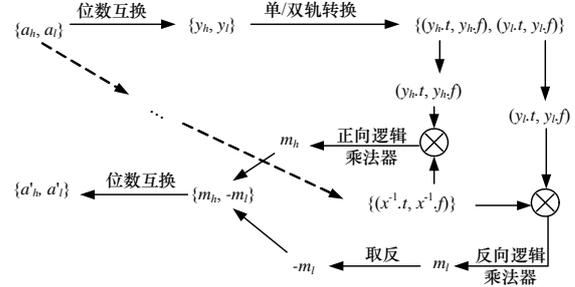


图 3 数据扰乱下的求逆运算过程

5 仿真实验

为了验证 S 盒的抗 DPA 攻击性能，按图 4 所示的流程建立仿真平台。用 5 000 个随机数序列 $R(i)$ 和测试密钥先做异或操作得到随机数序列 $D(i)$ ，组成输入数据序列 $I(i)=\{D_0, 0, D_1, 0, \dots, 0, D_{4998}, 0, D_{4999}\}$ ，以每 100 ns 一个数据的频率激活 S 盒；以 10 ps 的采样频率记录下 S 盒输出的瞬态功耗值。这样，与 5 000 个随机数

对应的有效工作时间内 (10 ns) 就会得到 1 000 个瞬态功耗值 $p_i(t)$ ，即第 i 个随机数在时间采样点 t 的瞬态功耗值 p 。于是得到与采样时间点 t 对应的 5 000 个随机数的瞬态功耗值构成的集合为 $P(t)=\{p_i(t) | \forall i=1, 2, \dots, 5000\}$ ，其中， $t=0,$

$1, \dots, 999$ 。与密钥相关的输入序列汉明差的求取过程如下：将 5 000 个随机数 $R(i)$ ，分别与 256 个假设密钥 $Kx=0, 1, \dots, 255$ 做异或操作，得到 256 组随机数的集合，利用 VC 程序计算出每个随机数与数据“0”的汉明距离差。这样就获得与 256 个假设密钥对应且包含 5 000 个汉明差集合： $H(k)=\{h_i(k) | \forall i=1, 2, \dots, 5000\}$ ，其中， $k=0, 1, \dots, 255$ 。

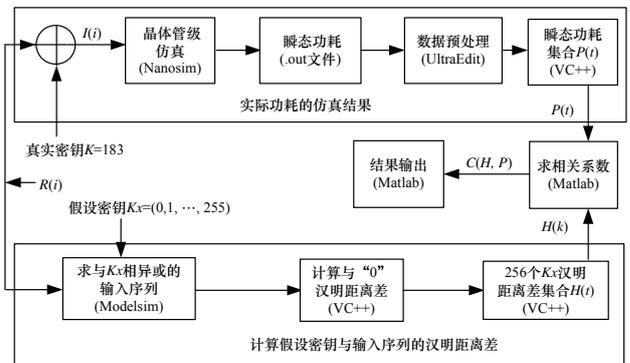


图 4 S 盒的 DPA 仿真攻击流程

利用 Matlab 编写相关脚本实现泊尔松相关系数公式，得

到每个时间采样点 t 在不同假设密钥 k 下,瞬态功耗输出 $P(t)$ 与数据输入汉明差 $H(k)$ 的相关系数。利用 Matlab 中的画图功能,得到 256 条与假设密钥相对应的时相关系数的曲线图。根据曲线图确定 256 000 个相关系数中的最大值所在的曲线后,该曲线所对应的密钥就是 S 盒加密操作密钥。

笔者在 1st Silicon 的 0.25 μm TNP CMOS 工艺下,设计得到局部插入双轨逻辑的全定制 AES S 盒的晶体管级电路。利用 Synopsys VCS/Nanosim 工具,在 2.5 V 和 25 $^{\circ}\text{C}$ 条件下进行 HSPICE 功耗仿真测试。利用上述 S 盒的 DPA 仿真攻击平台,对局部双轨 S 盒所做的 DPA 攻击测试结果如图 5 所示。可见,真实密钥($K=183$)对应的相关系数曲线的最高值被完全掩埋,密钥没有被破解。

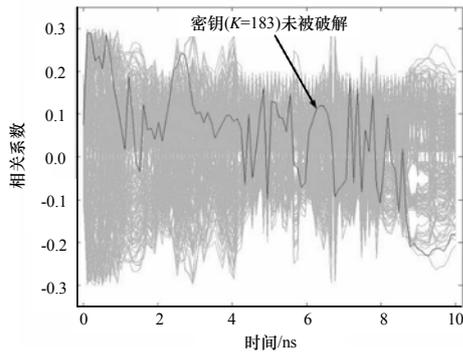


图 5 局部双轨 S 盒的抗 DPA 攻击测试结果

6 结束语

本文从异步电路设计方法学角度对抗 DPA 攻击方法进行研究,证明在单轨电路中局部采用异步双轨电路和随机数控制下的数据扰乱机制对改善电路的抗差分功耗分析攻击性

能是有利的,但是在具体设计中,如何权衡诸如面积、性能、功耗等方面的影响,找到最优的实现方案,及如何对整个设计效果进行量化,还有待深入研究。

参考文献

- [1] 谢满德, 沈海斌, 竺红卫. 对智能卡进行微分功耗分析攻击的方法研究[J]. 微电子学, 2004, 34(6): 609-613.
- [2] Schramm K, Paar C. IT Security Project: Implementation of the Advanced Encryption Standard(AES) on a Smart Card[C]//Proc. of ITCC'04. Piscataway, NJ, USA: [s. n.], 2004.
- [3] 曾永红, 邹雪城, 刘政林, 等. 低功耗 AES S 盒的 ASIC 设计与实现[J]. 微电子学, 2007, 37(4): 610-614.
- [4] Satoh A, Morioka S, Takano K, et al. A Compact Rijndael Hardware Architecture with S-box Optimization[C]//Proc. of the 7th International Conf. on the Theory and Application of Cryptology and Information Security. Gold Coast, Australia: [s. n.], 2001.
- [5] Zeng Yonghong, Zou Xuecheng, Liu Zhenglin, et al. A Low-power Rijndael S-Box Based on Pass Transmission Gate and Composite Field Arithmetic[J]. Journal of Zhejiang University: SCIENCE A, 2007, 8(10): 1553-1559.
- [6] 韩 军, 曾晓洋, 汤庭整. 基于时间随机化的密码芯片防攻击方法[J]. 计算机工程, 2007, 33(2): 6-8.
- [7] Shang D, Burns F, Bystrov A, et al. High-security Asynchronous Circuit Implementation of AES[J]. IEE Proceedings: Computers and Digital Techniques, 2006, 153(2): 71-77.

编辑 顾姣健

(上接第 19 页)

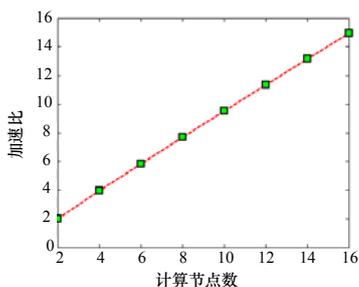


图 9 并行标记性能测试结果

6 结束语

本文提出一种新的基于游程的顺序扫描式区域标记算法,同时适用于串行标记和并行标记。通过实验分别对算法的串行标记性能以及并行标记性能进行了测试。另外,本文的间接关联构架思想不止适用于游程这种图像表达方式,其他的图像表达方式也可借鉴该思想从而形成相应的顺序式扫描标记算法。

参考文献

- [1] Shima Y. A High Speed Algorithm for Propagation-type Labeling Based on Block Sorting of Runs in Binary Images[C]//Proc. of the

- 10th International Conference on Pattern Recognition. [S. l.]: IEEE Press, 1990: 655-658.
- [2] Chang Fu, Chen Chun-Jen, Lu Chi-Jen. A Linear-time Component-labeling Algorithm Using Contour Tracing Technique[J]. Computer Vision and Image Understanding, 2004, 93(2): 206-220.
- [3] Rosenfeld A, Pfaltz J L. Sequential Operations in Digital Picture Processing[J]. Journal of ACM, 1966, 13(4): 471-494.
- [4] Stefano L D, Bulgarelli A. A Simple and Efficient Connected Components Labeling Algorithm[C]//Proc. of Int'l Conference on Image Analysis and Processing. [S. l.]: IEEE Press, 1999: 322-327.
- [5] Suzuki K. Linear-time Connected-component Labeling Based on Sequential Local Operations[J]. Computer Vision and Image Understanding, 2003, 89(1): 1-23.
- [6] Dillencourt M B, Samet H, Tamminen M. A General Approach to Connected Component Labeling for Arbitrary Image Representations[J]. Journal of ACM, 1992, 39(2): 253-280.
- [7] 徐利华, 陈早生. 二值图像中的游程编码区域标记[J]. 光电工程, 2004, 31(6): 63-65.
- [8] 陈国良. 并行算法的设计与分析[M]. 北京: 高等教育出版社, 2002.

编辑 张 帆

