

## 针对 AES 第一轮的汉明重代数攻击研究

郑媛媛<sup>1</sup>, 王 韬<sup>1</sup>, 赵新杰<sup>1</sup>, 侯志奇<sup>2</sup>

(1 军械工程学院 计算机工程系, 河北 石家庄 050003; 2 河北银行学校, 河北 石家庄 050081)

**摘 要:** 将差分功耗分析的汉明重量模型与传统的代数攻击相结合, 实现了针对 128 位密钥的 AES 密码算法第一轮的功耗代数攻击. 在攻击实验中, 改进了汉明重量函数, 并证明了利用此函数能够通过进一步计算的相关系数  $r$  明显区分出正确密钥字节与错误密钥字节, 在最短时间内获得正确的真实的全部密钥字节, 对比其他同类研究更具适用性和高效性.

**关键词:** AES; DPA; Hamming-Weight; 汉明重代数攻击; 相关系数

**中图分类号:** TP309

**文献标识码:** A

**文章编号:** 1000-7180(2011)07-0082-04

## Research in HW Algebraic Attack on AES First Round

ZHENG Yuan-yuan<sup>1</sup>, WANG Tao<sup>1</sup>, ZHAO Xin-jie<sup>1</sup>, HOU Zhi-qi<sup>2</sup>

(1 Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China;

2 HeBei Banker School, Shijiazhuang 050081, China)

**Abstract:** Combine the Hamming-Weight model of DPA with traditional algebraic attack, and achieve the power algebraic attack on the first round of AES-128. In the attack experiment, improve the function of Hamming-Weight, and prove that it can evidently distinguish the right key bytes from the wrong ones by further computed correlation coefficient  $r$ , and then acquire all the true key bytes in certain time. It is experimentally proved that this method is more applicable and more effective than other corresponding research.

**Key words:** AES; DPA; Hamming-Weight; HW algebraic attack; correlation coefficient

### 1 引言

基于代数的密码分析方法立足于分组密码算法本身, 通过求解表示密码算法的以密钥位未知数的变量的稀疏二次方程组, 实现直接攻击密码算法的目的, 然而由于方程组复杂, 使得完全求解方程组不可行. 基于功耗的密码分析方法立足于分组密码算法实现过程中的功耗泄露信息漏洞, 通过发现与密钥相关的功耗信息, 进一步分析, 间接达到获取密钥的目的, 这种方法的适用性有时会受到密钥多变或访问策略改变等攻击环境的影响. 为此, 文中将对 AES 第一轮中泄露的功耗/汉明重量信息进行分析, 生成线性代数方程组, 进一步利用代数攻击的方法, 获取 AES 的 128 位密钥.

### 2 AES 密码算法

AES 是一个基于有限域运算的迭代密码, 有 128 位、192 位和 256 位三种密钥版本. 不同的密钥版本只是采用了不同的密钥扩展算法和更多的加密轮数, 其中 128 位的密钥版本的密码算法需要进行 10 轮迭代. 文中不再完整描述 AES 密码, 仅描述研究所用到的 AES 密码的相关特性. AES 密码算法的迭代过程如图 1 所示, 该图仅表示了第一轮和最后一轮的代数运算. 其余中间各轮, 如第  $i$  轮迭代根据 16 字节的输入状态  $x^{(i)}$  和一个 16 字节的子密钥  $K^{(i)}$ , 产生一个 16 字节的输出状态  $x^{(i+1)}$ . 除最后一轮之外, 每一轮迭代运算都包括对输入  $x^{(i)}$  的以下四个的代数运算: 字节代换 (SubBytes), 行移位 (ShiftRows), 列混淆 (Mix-

收稿日期: 2010-09-08; 修回日期: 2010-10-28

基金项目: 国家自然科学基金项目(60772082); 河北省自然科学基金数学研究专项(08M010)

Columns), 然后和轮子密钥  $K^{(i)}$  作异或运算 (AddRoundKey). 其中图 1 第一轮  $x_{ij}^{(0)} = p_{ij}$ .

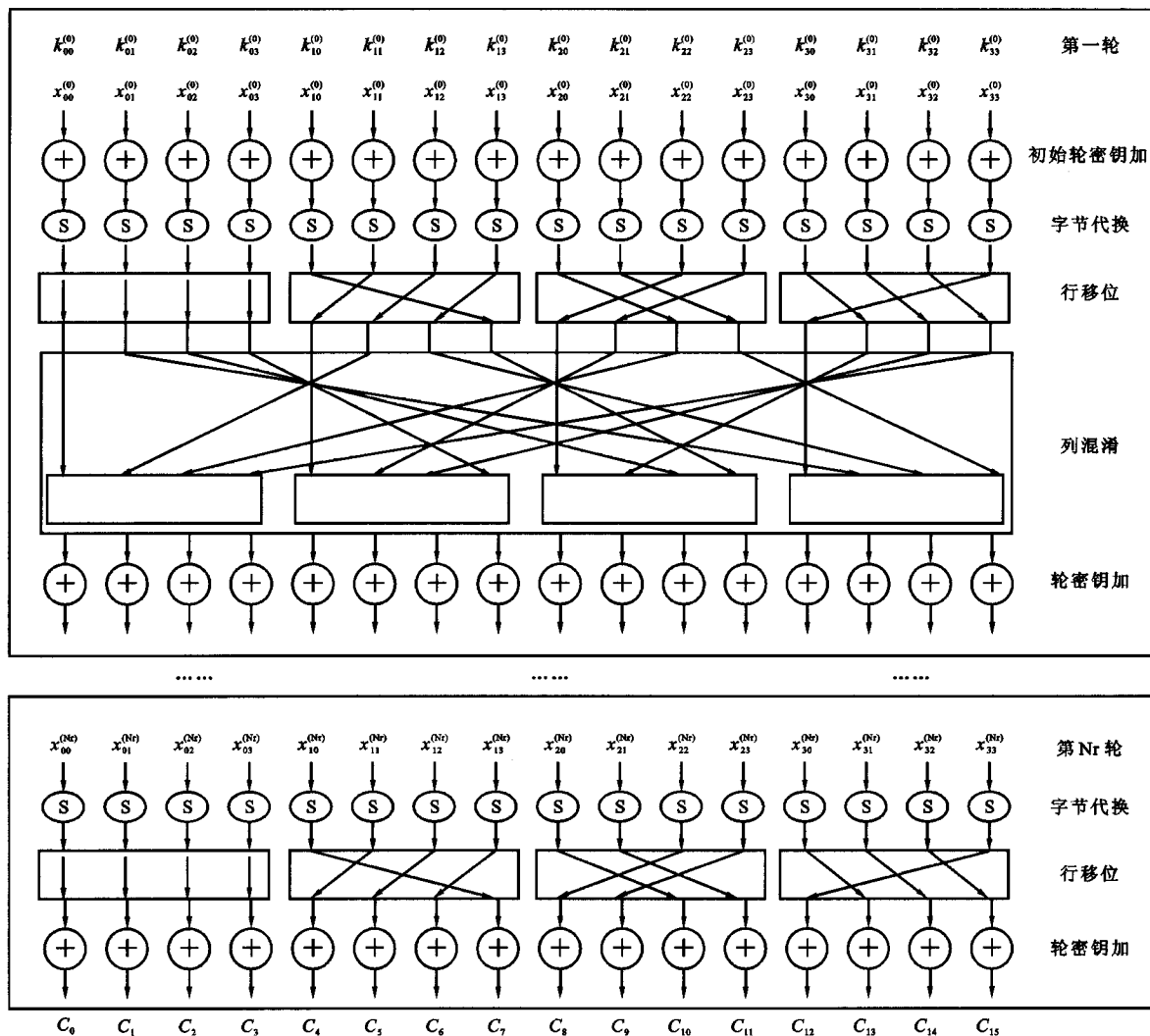


图1 AES 密码算法第一轮和最后一轮执行的代数运算

### 3 功耗密码分析及基于汉明重量的代数攻击

功耗密码分析包括简单功耗分析和差分功耗分析,其本质都是利用硬件(芯片或智能卡)在执行密码操作过程中泄露的与密钥相关的功耗信息,通过进一步复杂的分析计算,最终获得较小的候选密钥空间,甚至是唯一的真实密钥。

执行密码操作的硬件是由 CMOS 单元构成的逻辑电路。该硬件的功耗可以分为两部分:一是静态功耗  $P_{\text{stat}}$ ,即逻辑单元在没有转换行为的情况下必然消耗的功率;二是动态功耗  $P_{\text{dyn}}$ ,逻辑单元进行内部信号或输出信号翻转的情况下消耗的功率。因此,逻辑单元的总功耗就是  $P_{\text{stat}}$  和  $P_{\text{dyn}}$  之和。对于执行密码操作的硬件来说,往往  $P_{\text{stat}}$  相同的,不同操作(是否发生翻转)的  $P_{\text{stat}}$  不同,而不同的操作间接反

映出来的就是密钥的相关信息。因此,在既定明文的情况下,根据加密过程中泄露的功耗信息刻画功耗泄露曲线,就可以获得与之匹配的真实密钥。简单功耗分析(SPA)<sup>[1]</sup>和差分功耗分析(DPA)<sup>[2-3]</sup>的区别就在于利用的不同功耗信息,前者利用的是加密过程中直接测量的实时功耗信息刻画了功耗泄露曲线,即以时间为横轴的连续的功耗信息,攻击者的目标是找到与这一条功耗曲线匹配的密钥;后者利用的是密码设备功率消耗的数据依赖性,即利用大量的功耗曲线分析固定时刻的以所处理数据(通常为明文字节及密钥字节)为自变量的功耗函数,具有差分的性质。

基于汉明重量泄露模型的旁路攻击<sup>[3]</sup>是利用功耗分析另一种代数攻击实现形式。这一技术目前已应用于 PRESENT 和 AES 分组密码。文献[4]提出了利用汉明重量泄露模型的代数旁路攻击,文献[5]

又针对更加复杂的 AES 密码算法实施了该类攻击。

在他们的实验中利用了密码算法 AES 所有轮的泄露信息,相比仅利用了 AES 第一轮和最后一轮的差分功耗分析,其实验结果能够在一次加密测量后就能够恢复密钥。然而,其大部分实验结果都是建立在已知汉明重量的基础上,着重对离线阶段的方程组求解方法进行阐述。在实际应用方面还有待改进。

#### 4 攻击实现

虽然国外研究学者在功耗旁路分析领域(包括差分功耗分析和相关功耗分析)已进行了深入研究,对汉明重量与密钥的关系研究的十分成熟,但是对于汉明重量的代数攻击研究较少。文中实验的攻击对象是运行于计算机中的 AES 分组密码,考虑到后续的实验以及实验设备有限,因此利用汉明重量模拟差分功耗。文中实验分析针对的是 AES 第一轮的字节代换操作泄露的汉明重量。

##### 4.1 攻击环境

攻击所用的计算机性能如表 1 所示。

表 1 实验用计算机性能

| 计算机性能指标 | 型号                            |
|---------|-------------------------------|
| CPU     | Intel Mobile Core 2 Duo T7250 |
| 一级缓存    | 8 路组相连 2 * 32KB               |
| 内存      | DDR2 1024MB                   |

攻击所用的编程平台为 Visual Studio .NET2005,实现了 AES 密码算法及 SAT 求解器,成功地恢复了 128 位 AES 密钥。

##### 4.2 关键技术

实验中选定的分析目标为 AES 第一轮的字节代换操作,因此在初始密钥异或操作后,输出值为

$K \oplus P$ ,其中  $K$  为初始密钥, $P$  为明文。同时  $K \oplus P$  也将作为第一轮字节代换操作的输入,其输出为  $S(K \oplus P)$ ,假定汉明重量函数为:

$$H = K \oplus P \oplus S(K \oplus P) \quad (1)$$

首先,分别假设  $K$  的每一个字节  $K[i], i \in [0, 15]$ 。例如假设  $K[i]$  为 0x00,  $P$  已知,代入式(1)得到预测的汉明重量  $H$ 。同理,在  $N$  个样本下可得到  $N$  个  $H$ ,依次将  $K[i]$  的所有可能值代入式(1),得到  $N * 2^8$  个  $H$  值;形成  $N * 2^8$  矩阵  $HW$ 。PO 是在对  $N$  个样本进行加密的过程中,在选定的 32 个测试点获得的实际功耗信息(文中用计时信息来仿真功耗信息)构成的  $N * L$  矩阵,其中  $0 \leq L \leq 31$ 。选取  $HW$  矩阵的一列(即  $K[i]$  为某猜测值时,对应第一轮字节代换操作时的汉明重量),同功耗矩阵  $PO$  的每一列进行关联分析。如果是猜测密钥字节是正确的,那么它和相应正确的字节代换操作的功耗点成正比,那么根据 Pearson 相关性系数  $r$  公式, $r$  值是最大的,除此以外的  $r$  值都很小,接近于 0。 $K$  的每个猜测值得到  $L$  个  $r$  值,形成一条相关曲线:

$$r(<x_1, \dots, x_s>, <y_1, \dots, y_s>) = \frac{\sum_{s=1}^S (x_s - \bar{x})(y_s - \bar{y})}{\sqrt{\sum_{s=1}^S (x_s - \bar{x})^2} \sqrt{\sum_{s=1}^S (y_s - \bar{y})^2}} \quad (2)$$

其中,  $x_i \in HW, y_i \in PO$ 。

对  $K[i]$  的其它可能值进行相关分析,最终得到 256 条相关曲线;观察曲线中存在最大尖峰的曲线,其对应的  $K$  值就是正确的密钥值。

##### 4.3 关键模块

攻击程序由下述模块构成: AES 密码算法实现模块、实际“功耗”点采集模块、分析模块、验证模块。各模块构成示意图如图 2 所示。

攻击想定:攻击在已知明文的假定情况下实施的,且采用式(1)代替实际功耗信息。

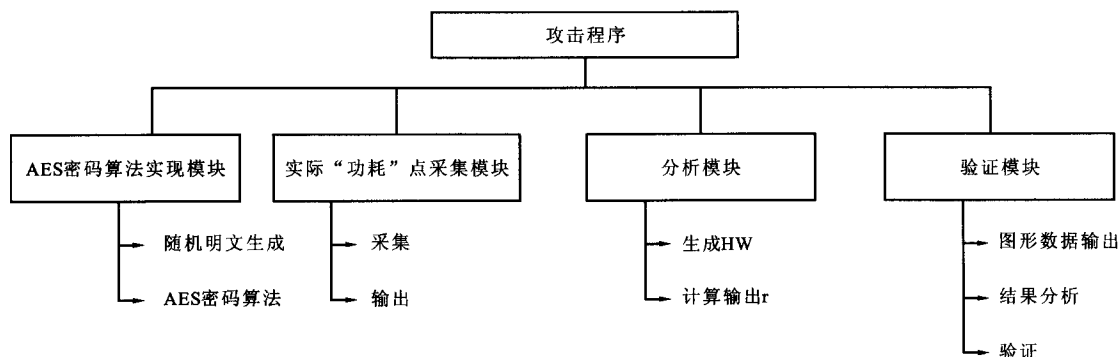


图 2 攻击程序功能模块

步骤 1: AES 利用明文产生器生成随机明文;

步骤 2: AES 执行加密过程, 采集模块负责采集实际功耗点信息, 构成矩阵  $PO$ ;

步骤 3: 分析模块产生所有可能的  $K$  值, 针对  $K$  的每一个字节  $K[i]$  及明文, 产生  $HW_{(N \times 2^8)}$  矩阵;

步骤 4: 分析模块结合功耗矩阵  $PO$ , 计算相关系数  $r$ ;

步骤 5: 验证模块针对各  $K[i]$  的所有可能值, 分别输出各采集点的相关系数  $r$ ;

步骤 6: 验证模块根据步骤 5 的输出结果, 确定每个密钥字节的真实值, 输出分析数据。

## 5 结果分析

图 3 为攻击过程中  $K[1]$  字节遍历各可能值的情况下在各测量功耗点的相关系数的分布, 其中纵坐标代表所计算各功耗点的相关系数  $r$  的值, 横坐标代表加密过程中采集的功耗点。此时真实的  $K[1]$  为  $0x05$ 。如图 3(a) 所示, 当  $K[1]=0x06$  时, 各实测功耗点的相关系数趋于平稳, 没有明显的尖峰; 如图 3(b) 所示, 当  $K[1]=0x05$  时, 在实测功耗点中有明显的尖峰, 与实际的  $K[1]$  相吻合。以此类推, 可以推出所有密钥字节  $K[i]$  的真实值, 进而获得真实密钥  $K$ 。

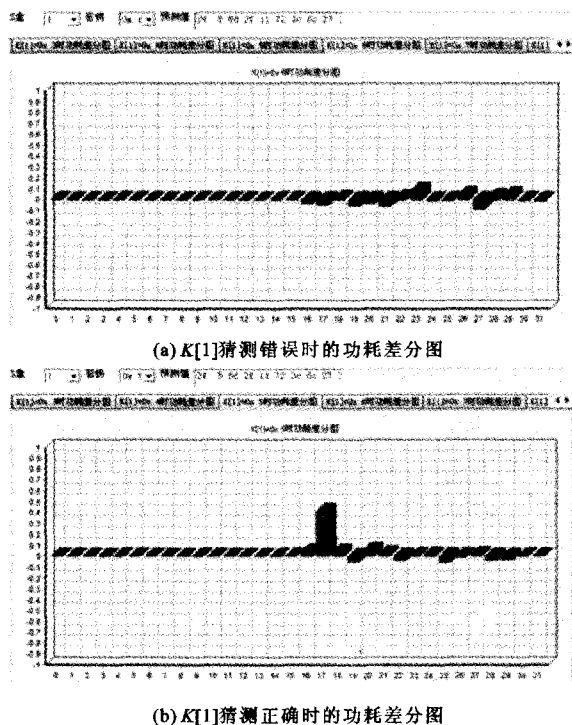


图 3 针对  $K[1]$  字节的功耗差分图

攻击实验证明了文中定义的汉明重量函数可以

间接反映密钥正确与否, 在已知明文的情况下, 可以推导出 128 位真实密钥值。

通过上述攻击仿真实验, 可以说明平均仅用 13 个随机明文, 针对不同密钥字节在第一轮对应采集 32 次功耗点, 就可简单获得正确与错误密钥的功耗差分曲线, 通过曲线的明显尖峰可判定得到正确的密钥字节。本实验不同于文献[5], 一方面通过构造相关系数的方法确定 16 个密钥字节, 更具有实用性; 另一方面, 改进了汉明重量函数, 可用更少明文, 多次测量, 达到同样的攻击效果, 但在一定程度上提高了攻击的效率。

## 6 结束语

文中将差分功耗分析的汉明重量模型与传统的代数攻击相结合, 在此基础上改进了汉明重量函数, 进行了针对 AES128 密码算法第一轮的攻击实验。实验证明, 文中提出的汉明重量函数可以较好的区分正确密钥字节与错误密钥字节, 使得在各功耗点实测值与猜测值的相关系数产生比较明显的差异, 最终可根据这些差异在较短时间内利用较少的测量次数确定正确的密钥字节。

### 参考文献:

- [1] Mangard S. A simple power analysis (SPA) attack on implementations of the AES key expansion [C]// ICISC2002. Seoul, Korea: Lecture Notes in Computer Science, 2002: 343–358.
- [2] Bogdanov A, Kizhvatov I, Pyshkin A. Algebraic methods in side-channel collision attacks and practical collision detection [C]// Indocrypt2008. Kharagpur, India: LNCS, 2008: 51–265.
- [3] Bogdanov A. Improved side-channel collision attacks on AES [C]// SAC2007. Ottawa, Canada: LNCS, 2007: 84–95.
- [4] Renaud M, Standaert F-X. Algebraic side-channel attacks [EB/OL]. [2010-03-13]. Cryptology ePrint Archive, report 2009/179, <http://eprint.iacr.org/2009/279>.
- [5] Renaud M, Standaert F X, Veyrat Charvillon N. Algebraic side-channel Attacks on the AES: Why Time also Matters in DPA [C]// CHES 2009, Switzerland: Lecture Notes in Computer Science, 2009: 97–111.

### 作者简介:

郑媛媛 女, (1981—), 博士研究生。研究方向为网络安全。