物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

基于Hamming weight和泄漏光子数的高级加密标准密码芯片光辐射分析攻击

王红胜 徐子言 张阳 陈开颜 李宝晨 吴令安

Attack on the advanced encryption standard cipher chip based on the correspondence between Hamming weight and the number of emitted photons

Wang Hong-Sheng Xu Zi-Yan Zhang Yang Chen Kai-Yan Li Bao-Chen Wu Ling-An

引用信息 Citation: Acta Physica Sinica, 65, 118901 (2016) DOI: 10.7498/aps.65.118901
在线阅读 View online: http://dx.doi.org/10.7498/aps.65.118901
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2016/V65/I11

基于Hamming weight和泄漏光子数的高级加密标准密码芯片光辐射分析攻击*

王红胜[1)†] 徐子言[1)] 张阳[1)] 陈开颜[1)] 李宝晨[1)] 吴令安[2)]

1) (军械工程学院信息工程系, 石家庄 050003)

2) (中国科学院物理研究所, 北京凝聚态物理国家实验室, 北京 100190)

(2016 年 1 月 26 日收到; 2016 年 3 月 4 日收到修改稿)

通过研究密码芯片运行时的光辐射迹及其数据依赖性, 建立了操作数汉明重量与泄漏光子数的对应关系, 提出了一种简单有效的针对高级加密标准 (AES) 加密算法的密码芯片光辐射分析方法. 根据密码芯片运行时的光泄漏特性, 利用时间相关单光子计数技术搭建了光辐射分析攻击实验平台, 在 AES 加密算法执行第一次的轮密钥加操作后和字节替换操作后分别进行光泄露信号采集, 对基于操作数 Hamming weight 和 AES 密码芯片泄漏光子数对应关系的密钥分析攻击方法的有效性进行了实验验证, 通过选择几组明文成功地破解了 AES 加密算法的密钥. 实验结果表明, 当密码芯片的泄露光子数与操作数的汉明重量呈近似线性关系时, 该种光辐射密钥分析攻击方法对 AES 密码芯片的安全性构成了严重的威胁.

关键词: 高级加密标准, 光辐射分析攻击, 密码芯片, 汉明重量

PACS: 89.20.Ff, 85.60.–q, 07.05.Kf, 03.67.Dd **DOI:** 10.7498/aps.65.118901

1 引 言

光旁路攻击是利用密码芯片运行时的光辐射特性或者某种光 (激光、紫外线等) 对密码芯片运行时的影响对其进行被动或者主动攻击的一种新型旁路攻击方法, 光旁路攻击可以分为光辐射分析攻击 [1−4] 和光故障注入攻击 [4].

自 Kocher 在 1996 和 1999 年发表具有开创性意义的文章——基于时间的旁路攻击 [5] 和基于功率的旁路攻击 [6] 以来, 旁路攻击成为密码分析学研究的一个重要领域. 相关旁路攻击手段 (如功耗分析攻击 [7]、电磁辐射攻击 [8]、故障注入攻击 [9] 等) 及多种分析方法 (如模板攻击 [10]、差分分析 [11] 等) 相继被研究. 传统的功耗、电磁等旁路攻击主要针对整个系统的信息泄漏进行分析, 2008 年首次提出光辐射分析攻击 [12], 其允许选择密码芯片硬件的特定部分进行光辐射分析, 使得光辐射分析攻击的选择性要远胜于功耗、电磁等分析攻击. 通过选取密码芯片特定位置/区域进行攻击可以得到信噪比非常好的光旁路信号, 这是由于光泄漏信号主要由我们所关心的密码芯片的相关指令操作及其操作数变化导致产生的. 然而, 由于文献 [12] 中的皮秒成像电路分析系统 (PICA) 的巨大实验花费和实验的复杂性, 使得光辐射分析攻击在当时没有被视为现实的威胁.

随着半导体技术和适合可见光、近红外等波段的硅基、铟镓砷、超导等单光子探测技术的快速发展 [13−15], 以及光辐射分析攻击新的方法和技术 (例如简单光辐射分析 [1,3]、差分光辐射分析 [1,2] 等) 的提出, 使用中低成本设备 [16−18] 开展密码芯片光辐射分析攻击成为可能和现实, 并为密码芯片光辐射分析攻击的进一步深入研究打下了基础.

本文以运行 AES 密码算法的单片机 AT89C52 作为密码芯片, 在对密码芯片光辐射迹及其数据依

* 国家自然科学基金 (批准号: 51377170, 11304007) 和河北省自然科学基金 (批准号: F2012506008) 资助的课题.

† 通信作者. E-mail: whswzx@aliyun.com

赖性分析的基础上, 研究了密码芯片操作数汉明重量和泄漏光子数之间的对应关系, 建立了密码芯片光辐射仿真模型, 提出了一种基于汉明重量和光子泄漏数对应关系的AES 密码芯片光辐射分析方法, 并进行了实验验证.

2 光辐射迹及其数据依赖性

2.1 密码芯片光辐射迹组成

如果采用时域光信号记录技术, 根据文献[4,16], 光辐射迹是指在密码芯片运行过程中, 利用单光子探测器和光子记录模块采样的光子数在时域上的分布, 它是光泄漏信号强度与时间的一个函数, 反映了运行过程中的密码芯片在各时间点上的光子泄露情况. 光辐射迹中既包含了对于破解密钥有用的信息, 也包含了部分噪声信号. 对于噪声信号的处理很大程度上决定了密钥分析的效率和精确性. 光辐射迹某一时间点的信号组成如下:

$$P = P_{\rm op} + P_{\rm da} + P_{\rm co} + P_{\rm no}, \tag{1}$$

在(1)式中, P为光辐射迹某一点的光子泄漏总量, $P_{\rm op}$为该点的操作依赖分量, $P_{\rm da}$为该点的数据依赖分量, $P_{\rm no}$是电子噪声, $P_{\rm co}$是一个常数分量. 其中, $P_{\rm op}$和$P_{\rm da}$是光辐射分析中最重要的分量, 尤其是$P_{\rm da}$. 这是因为光辐射分析攻击主要是利用了运行时密码芯片的光辐射迹依赖于其执行的运算和处理的数据, 执行不同的操作及处理不同的数据, 会导致产生不同的光辐射迹. 电子噪声$P_{\rm no}$主要由量化噪声、外部环境干扰、电源及时钟噪声等组成, 它导致密码芯片在运行程序和处理数据不变的情况下采集的光辐射迹仍然会出现不同. 为了提高信噪比并降低电子噪声对分析效率的影响, 一方面, 可以采用时间相关单光子计数(TCSPC)技术记录光子, 其具有比模拟信号记录技术更小的量化噪声; 另一方面, 因为$P_{\rm no}$服从正态分布$N(0,\sigma^2)$, 为使得期望值趋于0, 可以进行多次光信号采集, 用求平均值的方法减少电子噪声影响. $P_{\rm co}$主要是由与运行程序和处理数据没有关联的晶体管转换造成的, 一般认为是一个常量.

2.2 密码芯片光辐射信号仿真模型

开展密码芯片光辐射分析攻击, 经常需要将指令的操作数或者其变化映射为光子泄漏的数量. 对于某次攻击而言, 攻击者关心的是多次仿真所获得的光辐射迹之间的差异, 其绝对值在分析攻击中并无实际意义, 因此, 攻击者采用的仿真模型比较简单, 常用两类四种模型[4,19]. 多元模型: 汉明重量模型(Hamming-weight model)、汉明距离模型(Hamming-distance model). 二元模型: 比特模型(bit model)、零值模型(zero model). 实际攻击时采用哪一种仿真模型, 需要根据攻击对象(数据)的变化特点、密码芯片对密码算法的实现方式(软件实现、硬件实现)、攻击方法的使用等灵活选择.

令X, Y表示两个n位二进制数, 可以将X和Y分别看作一个具有n个元素的位向量(bitvector), $X, Y \in \{0,1\}^n$; x_i和y_i分别是X和Y的第i位二进制数, 则$x_i \in \{0,1\}$, $y_i \in \{0,1\}$, $i \in [0, n-1]$.

2.2.1 汉明重量模型

该模型假设密码芯片光子泄漏数量与被处理数据所等效的二进制数的各位“1”的个数成正比. 使用$HW(X)$表示X的汉明重量, 则有:

$$HW(X) = \sum_{i=0}^{n-1} x_i. \tag{2}$$

2.2.2 汉明距离模型

该模型假设密码芯片光子泄漏数量与被转换的先后两个数据所等效的二进制数的各对应二进制位“1”转换成“0”和“0”转换成“1”的总数成正比. 值X和Y的汉明距离可以表示为($\oplus$表示异或操作):

$$HD = HW(X \oplus Y) = \sum_{i=0}^{n-1} x_i \oplus y_i. \tag{3}$$

使用汉明距离模型进行密码芯片光辐射仿真时, 需要做出的假设是: 对于二进制数位, 所有“0”变“1”转换和“1”变“0”转换对于光子泄漏的贡献完全相同.

如果X的各二进制位均为“0”, 即$X = 0$, 那么, 在这种情况下, X变换为Y, Y的汉明重量模型与X变换为Y的汉明距离模型是等价的, 即$HW(Y) = HD(X, Y)$.

2.2.3 比特模型

比特模型非常简单, 对于值X, 其所等效的二进制数的某一位, 称为某一比特(bit). 该模型假设密码芯片光子泄漏数量与被处理数据所等效的二进制数被指定的某一位的值成正比. 例如, 仅考虑X的最低位x_0, 其比特模型即为$HW(x_0) = x_0$.

2.2.4 零值模型

该模型假设处理数值0所需要的光子泄漏要小于处理所有其他非零值. X 的零值模型为

$$ZV(X)=\begin{cases}0, & X=0\\ 1, & X\neq 0\end{cases}. \tag{4}$$

实际上, 上述模型是对被处理的数据对象在密码芯片上进行运算时导致的光子泄漏数量的一种相对估值和模拟, 具体采用哪一种模型, 除了上面所说的注意事项外, 还需与具体攻击模型相结合. 对于针对AES算法密码芯片的攻击模型而言, AES算法的攻击点(光泄漏点)一般选择在AES算法第一轮的轮密钥加输出/S盒输出或最后一轮S盒的输入, 如果针对的是字节分析攻击, 可以选择汉明重量模型或汉明距离模型.

2.3 密码芯片光辐射迹的数据依赖性

对密码芯片进行光辐射分析攻击, 我们主要关心光辐射迹中的数据依赖分量. 在文献[4,16]中, 为获取密码芯片AT89C52执行相同指令并操作不同数据的光泄漏特征, 我们让芯片执行指令MOV R7, A, 利用基于TCSPC技术的测量配置, 使硅基单光子探测器通过光纤对准芯片的R7寄存器, 对R7寄存器的光泄漏信号进行采集. 实验中参考了汉明仿真模型[4,16,19], 每次改变R7寄存器值前先将R7值设置为00(十六进制, 下同), 使R7寄存器值每次变换都是从00变换到某个数值; 然后将R7值分别改变为00, 01, 03, 07, 0F, 1F, 3F, 7F, FF, 对应寄存器R7依次翻转0—8位(二进制). 因此, 在这个实验中, R7寄存器值的汉明重量与汉明距离是相同的. 实验结果表明, 寄存器R7变换位数越多, 泄漏光子数越多, 数据变化(二进制数各位的变化)与密码芯片光子泄漏存在相关性, 如图1所示. 同时, 图1实验结果表明, 密码芯片的光泄漏与R7寄存器值的9种不同汉明重量存在依赖关系, R7寄存器值不同的汉明重量, 其泄露的光子数不同, 两者呈现出近似的线性关系. 该结论至关重要, 这意味着如果已经采集到R7寄存器泄露的光子数, 根据其值的大小, 可以判断R7寄存器值的汉明重量. 由于R7寄存器值是个8位二进制数, 其值有256种可能, 如果知道其汉明重量, 就可以缩小搜索范围, 建立一个与其汉明重量匹配的可能值的集合. 这也是基于汉明重量和光子泄漏数对应关系的AES光辐射分析攻击的理论和实验基础.

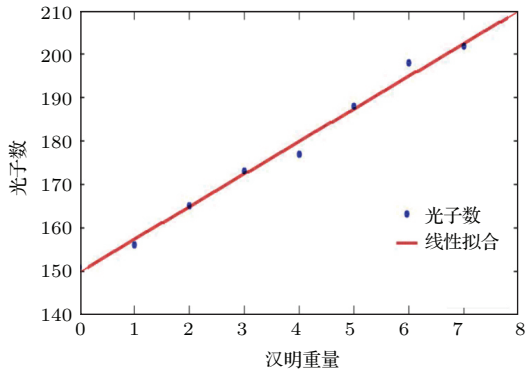

图1 R7寄存器9种不同汉明重量的平均光泄漏点状图及其线性拟合结果

Fig. 1. Dot chart and linear fitting result of mean photonic emission from R7 for the 9 different Hamming weights.

3 基于汉明重量和光子泄漏数对应关系的密钥分析方法

3.1 AES算法及光泄露点(中间值)选取

AES是美国国家标准与技术研究院批准的一个分组长度为128-bit的迭代型分组密码算法[19,20], 其针对一个4 × 4字节的明文矩阵进行操作, 称为状态矩阵. 根据密钥的长度为128-bit, 192-bit或256-bit, 分别称为AES-128, AES-192或AES-256. 对于AES-128十轮循环加密算法而言, 其使用128-bit密钥加密128-bit的明文分组, 数据和密钥均使用一个4 × 4的字节矩阵, 除了最后一轮不包括列混淆操作外, 每个循环包括四个不同的步骤[20](字节替换, 行移位, 列混淆, 轮密钥加), 此外, 在第一轮前进行轮密钥加操作. 在整个加密过程中, 原始密钥用于首轮循环前的轮密钥加操作, 后面循环的轮密钥由初始密钥衍生得到.

图2给出了光辐射分析攻击AES算法光泄漏点(AES算法的某个或某几个中间值)的选取, 其表示AES-128加密算法第一轮循环前的轮密钥加(实质是异或)操作和第一轮字节替换(又称为S盒变换)操作的流程. 在该加密过程中, 原始密钥k不变, 分别选取字节变换的输入(轮密钥加的输出)和输出(即S盒变换输出)作为两个光泄漏采集点.

对已知若干条明文分组$d_i(i=0,1,2,\cdots)$进行加密运算, 可分别得到该加密流程下明文第一个字节与原始密钥第一个字节异或操作后和S盒变换操作后输出值的汉明重量:

$$HW(d_{i,0}\oplus k_0)=HW(X_{i,0}), \tag{5}$$

$$HW(S(d_{i,0} \oplus k_0)) = HW(S_{i,0}), \qquad (6)$$

这里用 $HW()$ 表示汉明重量, $S()$ 表示上述 AES 算法过程中的 S 盒变换操作. (5) 式中 $d_{i,0}$ 表示明文分组 d_i 的第一个字节, k_0 表示原始密钥 k 的第一个字节, $HW(X_{i,0})$ 表示 $d_{i,0}$ 与 k_0 异或后值的汉明重量; (6) 式中 $HW(S_{i,0})$ 表示 $d_{i,0}$ 与 k_0 异或后再经 S 盒变换后值的汉明重量.

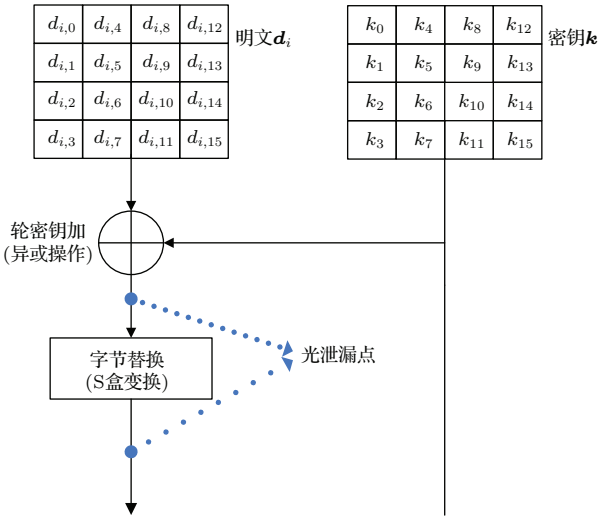

图 2 AES 算法光泄漏点 (中间值) 的选取

Fig. 2. The selected photonic emission points (intermediate points) on the AES algorithm.

3.2 基于汉明重量和光子泄漏数对应关系的 AES 密钥分析

假定明文 d_i 已知、密钥 k 未知, 下面实施对密钥 k 的分析攻击. 首先对密钥 k 第一个字节 k_0 进行分析. 采集 AES 密码芯片上述两个光泄漏点的光子数, 通过对照光子数与汉明重量的关系 (对应关系将在 4.2 节进行进一步详细说明), 确定出 $HW(X_{i,0})$ 和 $HW(S_{i,0})$ 的值. 由于明文 d_i 已知, 下面就可以对原始密钥 k 第一个字节 k_0 的可能值集合进行分析 (猜测). 对于 8 位的 k_0 而言, 所有可能的取值有 256 种 (k_0 = 0,1,2, ···, 255), 分别和明文分组 d_i 的第一个字节 $d_{i,0}$ 进行异或运算, 筛选出异或运算结果的汉明重量等于 $HW(X_{i,0})$ 的密钥, 得到一个密钥可能值集合 k_0'; 再对 k_0 可能值 (集合 k_0' 中的各元素) 和 $d_{i,0}$ 异或的结果进行 S 盒变换操作, 进一步得到 S 盒变换后值的汉明重量与 $HW(S_{i,0})$ 相等的密钥可能值, 即得到进一步缩小范围的密钥可能值集合 k_0''. 此时, 通过上述两步的筛选, k_0 可能的密钥值数量已经大大减少. 如果 k_0 密钥可能值集合 k_0'' 的元素个数大于 1, 则继续使用其他不同的明文, 重复进行上述两步操作, 对得到的密钥可能值集合 k_0'' 与上条明文确定的密钥可能值集合 k_0'' 进行求交集运算, 产生新的密钥可能值集合, 直到密钥可能值集合的元素个数为 1, 就可以得出密钥 k_0, 整个过程大概需要 2 条或者 3 条明文就可以确定出密钥 k_0. 以此类推, 通过对密钥 k 的其他字节和明文其他对应字节重复进行上述操作, 可以恢复出全部密钥.

基于汉明重量值和泄漏光子数对应关系的密钥分析方法如图 3 所示, 主要包括 4 个步骤.

步骤 (1) 中不再是传统的随机明文的旁路攻击, 而是采用选择明文加密的方式进行光辐射分析攻击. 其中 m 条明文用于采集密码芯片加密时的

基于汉明重量值和泄漏光子数对应关系的密钥分析

(1)选择m条明文进行加密(对每组明文采集n遍，求均值得到一条光辐射迹), 获得m条光辐射迹;
(2)对于m条光辐射迹, 根据汉明重量值和泄漏光子数的对应关系确定出各自光泄漏点中间值的汉明重量;
(3)攻击密钥的一个字节(以密钥第一个字节 k_0 为例说明), 初始化集合C(包含一个字节的256种组合);
(4)选择一条(第 i 条)明文加密对应的光辐射迹, 初始化集合A、B(为空集);
for $k_0 = 0$ to 255
{HW($X_{i,0}$) = HW($d_{i,0} \oplus k_0$);
if (HW($X_{i,0}$) = = 首次轮密钥加中间值的汉明重量值)保留k_0至集合A中; else丢弃k_0;}
number = 集合A中的元素个数;
for $j = 0$ to number -1
{HW($S_{i,0}$) = S(HW($d_{i,0} \oplus$A(j)));
if (HW($S_{i,0}$) = 首次字节变换中间值的汉明重量值)保留A(j)至集合B中; else丢弃A(j);}
求集合B与集合C的交集并保存至集合C; number = 集合C中的元素个数;
if (number = 1)集合C中的元素即为密钥的第一个字节k_0, 转到步骤(5);
else选择另一条明文加密的光辐射迹, 重复步骤(4),
(5)重复步骤(3)、(4), 对k_l (l = 1、2, ···, 15)进行分析，直至获得完整密钥

图 3 基于汉明重量值和泄漏光子数对应关系的密钥分析过程

Fig. 3. Analysis of the key based on the correspondence between the number of emitted photons and the Hamming weight.

光泄漏信号, 大多数情况下 m 取值为 2 或 3 就可以确定出密钥. 对每组明文采集 n 遍是为了更好地抑制电子噪声, 由于电子噪声呈正态分布, 可以采取求均值的方法减少电子噪声的干扰. 需要注意的是, 进行光泄漏信号采集时, 必须将光纤对准我们所关心的操作数在密码芯片上的位置 (区域). 通过步骤 (1), 得到 m 条光辐射迹.

步骤 (2) 中确定出各条光辐射迹中光泄漏点中间值的汉明重量. 由于密码芯片光辐射迹的数据依赖性 [4,16], 光泄漏点中间值 (例如 R7 寄存器值) 不同的汉明重量与泄漏光子数呈现出近似的线性关系, 因此, 可以建立二者之间的对应关系 (在 4.2 节进一步给出), 从而使用在步骤 (1) 获得的光辐射迹实验数据确定出两个光泄漏点中间值的汉明重量.

步骤 (3), (4) 针对密钥的某个字节, 得到满足两个光泄漏点中间值汉明重量的可能密钥值集合, 通过两步筛选能够将密钥可能值压缩于很小的范围内, 通过多条明文加密的光辐射迹 (例如 2 条或者 3 条) 就可以确定出该密钥字节.

步骤 (5) 主要是通过对密钥 k 的其他字节和明文其他对应字节重复进行步骤 (3), (4), 就可以恢复出密钥的其他字节, 进而得到完整的密钥.

4 针对 AES 密码芯片基于汉明重量和泄露光子数对应关系的光辐射分析攻击

4.1 实验测量配置及其质量评价

4.1.1 测量配置

以 AT89C52 密码芯片为待测芯片, 在其上运行 AES 加密算法. 为了更好地对光泄漏信号进行探测, 需要对 AT89C52 密码芯片进行开片处理 [16], 主要使用机械打磨和化学腐蚀的方法对待测芯片进行处理. 参考文献 [4,16] 使用了基于 TCSPC 的密码芯片光泄漏测量配置, 整个实验测量装置主要由 TCSPC 光信号记录模块 [21]、单片机、主控计算机、分析处理计算机、单光子探测器 (SPAD)、两个反相器和两个衰减器等组成, 实验测量配置如图 4 所示.

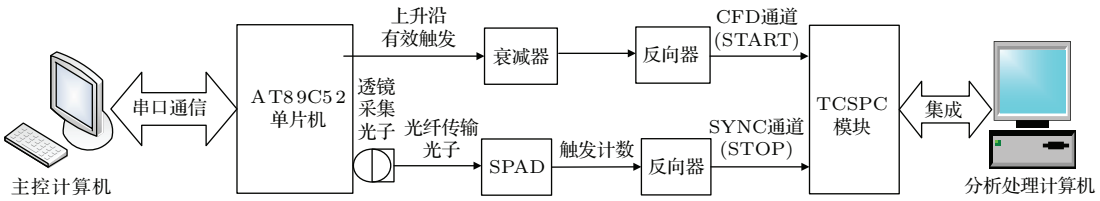

图 4 基于 TCSPC 光泄漏测量配置

Fig. 4. Setup for measuring the photonic emission based on TCSPC.

主控计算机通过 RS232 串行口给单片机发送相关指令, 以控制其执行相关程序和数据处理; 分析处理计算机主要保存光辐射迹并进行相关格式转换等处理; TCSPC 模块主要用于接收单光子探测器的输出, 完成密码芯片在运行时泄漏光子的计数并形成光辐射迹, 为后期的分析处理做准备; 使用硅基 SPAD 单光子探测器, 其俘获光子波长的范围为 400—1060 nm, 对可见光有较高的采集效率.

4.1.2 质量评价及噪声分析

可以从单光子探测器的选择、光信号的记录和处理、光纤和透镜的选择、微操作台设计、待测密码芯片的预处理、噪声分析等方面对测量配置的质量评价给出一个定性及定量的基本描述, 特别是可以使用光辐射迹中出现的噪声来对测量配置的质量进行刻画, 从而帮助改进测量配置, 进一步减少测量中的不确定性和误差, 提高光辐射分析的效率 [4].

根据文献 [4], 密码芯片光辐射迹中的主要噪声是电子噪声和转换噪声.

4.1.2.1 电子噪声

在光辐射分析攻击中, 当密码芯片执行相同的指令和处理相同的数据时, 重复测量在此期间密码芯片的光辐射迹, 实际测量的各光辐射迹会有所不同, 我们将这种情况下的光辐射迹的波动称为电子噪声. 现实当中, 每一次测量都会带来电子噪声, 其主要来源包括量化噪声、实验外部环境的干扰、电源及时钟.

1) 量化噪声

量化噪声是在光信号采集、探测和记录过程中由于光电转换、模数转换造成的. 实际的量化噪

声主要由单光子探测器和光子记录技术的分辨率决定, 分辨率越高, 量化噪声越小. 在采用适合的单光子探测器的前提下, 针对密码芯片光泄漏, 文献 [4,16] 验证了采用 TCSPC 技术的有效性; 同时, TCSPC 技术具有比模拟信号记录技术更小的量化噪声, 因而具有更好的信噪比 [21].

2) 实验外部环境的干扰

在密码芯片光泄漏采集过程中, 要求在暗室环境下, 并且周围尽量无震动等干扰, 以减少由此带来的对测量不必要的影响.

3) 电源及时钟

在密码芯片设计要求的范围内, 芯片工作电压越高、时钟频率越高, 运行时的密码芯片的光泄漏就越强 [4,16]. 在实验中, 有必要使用高质量的稳压电源, 同时, 使用能够产生并保持高度稳定时钟频率的时钟发生器.

让密码芯片执行相同的指令并处理相同的数据, 对其光辐射迹进行多样本量采样的实验分析结果表明 [4], 光辐射迹上我们所攻击的泄漏点的电子噪声呈现近似正态分布. 因此, 可以通过多次采样并求平均值的方法进一步消除测量的不确定性和误差.

4.1.2.2 转换噪声

在密码芯片运行过程中, 我们将“由指令执行和数据操作引起的但与实际攻击无关的晶体管转换活动所产生的光泄漏”称之为转换噪声 [4]. 例如, 如果我们只关心 R7 寄存器 (8 位二进制数, 1 个字节) 的最低数值位, 与该数值位相关的晶体管发生转换产生的光泄漏是有效有价值的光信号, 而该寄存器其余 7 位对应的晶体管发生转换产生的光泄漏则是转换噪声.

对光辐射分析攻击而言, 转换噪声的数量依赖于所攻击的对象, 依赖于测量配置, 依赖于密码芯片的结构. 通过优化单光子探测器的选择和光路系统的设计等测量配置, 光辐射分析攻击可选取密码芯片的特定区域, 以有效降低转换噪声.

4.2 建立汉明重量和泄漏光子数的对应关系

根据文献 [4,16], 当密码芯片执行相同的指令并操作不同的数据时, 密码芯片的光泄漏和操作数 (例如 R7 寄存器的值) 的汉明重量存在着近似线性关系. 为实施基于汉明重量和泄漏光子数对应关系的 AES 密码芯片光辐射分析攻击, 需要首先建立操作数汉明重量与密码芯片泄漏光子数的对应关系. 具体实验过程为: 以 R7 数据寄存器为测试对象, 运行 MOV R7, A 指令进行光泄漏分析, 整个过程让光纤和透镜对准密码芯片上 R7 数据寄存器的位置, 工作电压选用 6.4 V 的电压值, 核心被测代码如下, 时间是 4 μs:

```
NOP          1 μs
MOV R7, A    1 μs
XRL P1, #08 H  2 μs
```

在实验中设定 TCSPC 模块的单次时间周期为 5 μs, 实际有效周期是 4 μs, 每次采集周期中光信号根据到达时间的先后分布在 4096 个时间通道中, 由于需要建立操作数 R7 寄存器值的汉明重量与泄露光子数的对应关系, 需要在给 R7 寄存器送入数值前对其进行清零操作 (上述核心被测代码未包含该指令). 对每个样本进行重复采集 10 min. 对于 R7 寄存器而言, 数据存储形式为一个 8 位的二进制数, 且各位之间相互独立, 故可能的值有 $2^8 = 256$ 种, 其汉明重量有 9 种可能 (即 0, 1, 2, 3, 4, 5, 6, 7, 8). 实验中我们将这 256 种取值分别送至 R7 寄存器, 对 256 个值分别送 2 次, 因此, 实验中总共采集 512 个光辐射迹样本. 根据 R7 寄存器数据汉明重量的值对各光辐射迹进行平均化处理, 选择光辐射迹中与 R7 数据处理相关的时间通道 (1119 时间通道至 1122 时间通道), 对其进行放大处理得到图 5.

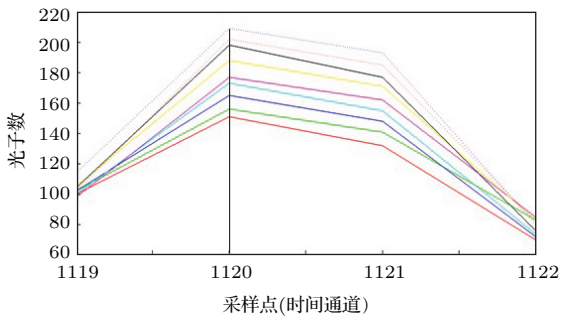

图 5 (网刊彩色) R7 寄存器 9 种汉明重量的平均泄漏轨迹

Fig. 5. (color online) Mean emission traces from the R7 register for 9 different Hamming weights.

从图 5 可明显看出时间通道 1120—1121 区间的光子泄露数量随操作数 R7 的不同汉明重量发生变化的情况, 从上往下, 9 条光辐射迹对应的汉明重量依次是 8, 7, 6, 5, 4, 3, 2, 1, 0, 随着操作数 R7 汉明重量的增加, 密码芯片泄漏的光子数增多. 效果较为明显的时间通道为 1120 通道, 故以 1120 通道为参考时间点, 从中我们可以得到操作数 R7 的汉明重量与泄漏光子数的对应关系, 如表 1 所列.

表 1 汉明重量值与泄漏光子数的对应关系

Table 1. Correspondence between the number of photons emitted and the Hamming weight.

汉明重量值	0	1	2	3	4	5	6	7	8
光子数	148—150	153—156	161—163	169—171	175—177	185—186	194—196	200—202	209—211

4.3 通过选择明文的 AES 光辐射分析攻击

如表 2 (除明文用十六进制表示外, 其他用十进制表示) 所列, 通过 2 组明文就可以获得密钥的首字节. 实验中, 使用 R7 寄存器保存图 2 所示的 AES 加密流程中不同光泄露点的 2 个中间值 (异或的结果和 S 盒变换的结果), 通过实验分别采集到 d_0 和 d_1 两条明文的首字节 (分别是十六进制表示的 $0x00$ 和 $0x$AA) 在异或后和 S 盒变换后泄漏的光子数, 根据上述给出的泄漏光子数与汉明重量的对应关系, 得到其相应的中间值 (泄露点) 的汉明重量值, 进而分别筛选出缩小范围的两个密钥可能值集合, 粗体为两个密钥可能值集合的重叠部分.

表 2 通过选择明文的 AES 光辐射分析攻击

Table 2. AES photon emission analysis attack based on selected plain texts.

组别	明文 (十六进制)	异或后光子数	异或后汉明重量值	S 盒变换后光子数	S 盒变换后汉明重量值	密钥可能值
d_0	$0x$0000000000000000	185	5	171	3	47, **93**, 94, 103, 118, 158, 171
d_1	$0x$AA00000000000000	202	7	170	3	87, **93**

然后, 对两条明文首字节经上述处理得到的两个密钥可能值集合进行求交集运算, 可以确定出密钥的第一个字节为十进制数 93, 其十六进制表示为 "$0x5d$".

按照上述方法, 对明文的后面字节进行类似处理, 可以得到完整的密钥.

实际上, 图 3 所示的基于汉明重量和光子泄漏数对应关系的密码芯片光辐射分析方法还可以进一步优化. 对于图 2 所示的 AES 加密流程中的 2 个中间值 (异或的结果及 S 盒变换的结果) 的汉明重量, 当处理密钥 k 的某个字节 k_i 时, 考虑到极端情况, 例如异或操作结果的汉明重量为 0 或者 8, 那么, 一条明文就足以破解密钥的对应字节, 这可以极大地缩小搜索范围.

5 结 论

运行状态的密码芯片的光辐射迹与被处理的操作数之间存在着相关性, 即所谓的光辐射迹的数据依赖性. 借助于汉明仿真模型, 当密码芯片泄露光子数与操作数的汉明重量呈近似线性关系时, 可以采用基于操作数汉明重量和泄漏光子数对应关系的密钥分析方法实施 AES 密码芯片光辐射分析攻击. 实验表明, 选择 AES 算法第一次异或后和 S 盒变换后的结果作为中间值和光泄漏信号采集点, 通过 2 条或多条已知明文, 结合汉明重量与泄漏光子数对应关系, 获得相关中间值的汉明重量, 就可以反推并破解密钥, 实验结果验证了方法的可行性和密钥的正确性. 下一步将对该方法进行优化, 以缩小搜索范围, 提高攻击效率, 并结合其他光辐射分析攻击 (简单光辐射分析、差分光辐射分析) 的研究, 进行攻击效率对比和评估; 同时, 改进实验测量装置, 提高光辐射信号信噪比和采集效率.

参考文献

[1] Krämer J, Kasper M, Seifert J P 2014 *19th Asia and South Pacific Design Automation Conference* Singapore, Republic of Singapore, January 20–23, 2014 p780

[2] Krämer J, Nedospasov D, Schlosser A, Seifert J P 2013 *Constructive Side-Channel Analysis and Secure Design* (Berlin: Springer-Verlag) p1

[3] Schlosser A, Nedospasov D, Krämer J, Orlic S, Seifert J P 2013 *J. Cryptogr. Eng.* **3** 3

[4] Wang H S 2015 *Ph. D. Dissertation* (Shijiazhuang: Ordnance Engineering Collage) (in Chinese) [王红胜 2015 博士学位论文 (石家庄: 军械工程学院)]

[5] Kocher P 1996 *Annual International Cryptology Conference* California, August 18–22, 1996 p104

[6] Kocher P, Jaffe J, Jun B 1999 *Annual International Cryptology Conference* California, USA, August 15–19, 1999 p388

[7] Hnath W 2010 *Ph. D. Dissertation* (Massachusetts: Worcester Polytechnic Institute) (in USA)

[8] Mulder E D 2010 *Ph. D. Dissertation* (Leuven: Katholieke Universiteit) (in The Kingdom of Belgium)

[9] Biham E, Shamir A 1997 *Annual International Cryptology Conference* Santa Barbara, California, USA, August 17–21, 1997 p513

[10] Wang T, Zhao X J, Guo S Z, Zhang F, Liu H Y, Zheng T M 2012 *Chin. J. Comput.* **35** 325 (in Chinese) [王韬, 赵新杰, 郭世泽, 张帆, 刘会英, 郑天明 2012 计算机学报 **35** 325]

[11] Kircanski A, Youssef A M 2010 *3th International Conference on Cryptology in Africa* Stellenbosch, South Africa, May 3–6, 2010 p261

[12] Ferrigno J, Hlavá M 2008 *IET Infor. Secur.* **2** 94

[13] Wang Y J, Ding T, Ma H Q, Jiao R Z 2014 *Chin. Phys. B* **23** 060308

[14] Liang Y, Zeng H P 2014 *Sci. China: Phys. Mech. Astron.* **57** 1218

[15] Sun Z B, Ma H Q, Lei M, Yang H D, Wu L A, Zhai G J, Feng J 2007 *Acta Phys. Sin.* **56** 5790 (in Chinese) [孙志斌, 马海强, 雷鸣, 杨捍东, 吴令安, 翟光杰, 冯稷 2007 物理学报 **56** 5790]

[16] Wang H S, Ji D G, Gao Y L, Zhang Y, Chen K Y, Chen J G, Wu L A, Wang Y Z 2015 *Acta Phys. Sin.* **64** 058901 (in Chinese) [王红胜, 纪道刚, 高艳磊, 张阳, 陈开颜, 陈军广, 吴令安, 王永仲 2015 物理学报 **64** 058901]

[17] Zhang L B, Kang L, Chen J, Zhao Q Y, Jia T, Xu W W, Cao C H, Jin B B, Wu P H 2011 *Acta Phys. Sin.* **60** 038501 (in Chinese) [张蜡宝, 康琳, 陈健, 赵清源, 郑涛, 许伟伟, 曹春海, 金飚兵, 吴培亨 2011 物理学报 **60** 038501]

[18] Liu Y, Wu Q L, Han Z F, Dai Y M, Guo G C 2010 *Chin. Phys. B* **19** 080308

[19] Mangard S, Oswald E, Popp T (translated by Feng D G, Zhou Y B, Liu J Y) 2010 *Power Analysis Attacks* (Beijing: Science Press) pp1–129 (in Chinese) [Mangard S, Oswald E, Popp T 著 (冯登国, 周永彬, 刘继业 译) 2010 能量分析攻击 (北京: 科学出版社) 第 1—129 页]

[20] Hu X D, Wei Q F, Hu R 2011 *Applied Cryptography* (2nd Ed.) (Beijing: Electronic Industry Press) pp1–95 (in Chinese) [胡向东, 魏琴芳, 胡蓉编应用密码学 (第 2 版) (北京: 电子工业出版社) 第 1—95 页]

[21] Becker W (translated by Qu J L) 2009 *Advanced Time-Correlated Single Photon Counting Techniques* (Beijing: Science Press) pp1–126 (in Chinese) [Becker W 著 (屈军乐 译) 2009 高级时间相关单光子计数技术 (北京: 科学出版社) 第 1—126 页]

Attack on the advanced encryption standard cipher chip based on the correspondence between Hamming weight and the number of emitted photons*

Wang Hong-Sheng[1)†] Xu Zi-Yan[1)] Zhang Yang[1)] Chen Kai-Yan[1)]
Li Bao-Chen[1)] Wu Ling-An[2)]

1) (*Department of Information Engineering, Ordnance Engineering Collage, Shijiazhuang 050003, China*)
2) (*Institute of Physics and Beijing National Laboratory for Condensed Matter Physics, Chinese Academy of Sciences, Beijing 100190, China*)

(Received 26 January 2016; revised manuscript received 4 March 2016)

Abstract

The security of information transmission is of paramount importance in all sectors of society, whether civilian or defence related. In ancient times the encryption of secret messages was mainly realized by physical or chemical means, but this was later supplemented by mathematical techniques. In parallel, the breaking of enemy codes has also been a subject of intense study. To date, the only known absolutely secure means of encryption is through quantum cryptography. However, this still has to be implemented by equipment that is vulnerable to various physical attacks, so it is important to study these methods of attack, both for legitimate users and for the surveillance of criminal activities. Today, nearly all transactions have to be realized through the computer and much effort has been devoted to cracking the software. However, little attention has been paid to the hardware, and it has only recently been realized that computer chips themselves can leak sensitive information, from which a code may even be deciphered.

By studying the photonic emission and the data dependency of a cryptographic chip during operation, the correspondence between the Hamming weight of the operand and the number of photons emitted may be established, based on which a simple and effective method is proposed to crack the Advanced Encryption Standard (AES) cipher chip. An experimental platform has been set up for measuring and analyzing the leaked photonic emission using time-correlated single-photon counting. An AT89C52 microcontroller implementing the operation of the AES cipher algorithm is used as a cipher chip. The emitted photons are collected when the first AddRoundKey and SubBytes of the AES encryption arithmetic are executed, and their respective numbers are found to have a linear relationship with the operand Hamming weight. The sources of noise affecting the photon emission trace have been analyzed, so that the measurement error and uncertainty can be reduced effectively. With the help of our Hamming weight simulation model, by selecting one or several groups of plain text and comparing the corresponding relationship between the Hamming weight of the intermediate values and the number of photons emitted by the cipher chip, the key of the AES encryption algorithm has been successfully recovered and cracked. This confirms the effectiveness of this method of attack, which can therefore pose a severe threat to the security of the AES cipher chip. For the next step in the future, our method will be optimized to narrow the search range, and also combined with other photonic emission analysis attacks (such as simple photonic emission analysis and differential photonic emission analysis) to improve the efficiency. A comparison and evaluation of the various methods will be made. At the same time, our current experimental configuration will be improved to obtain a better collection efficiency and signal-to-noise ratio.

Keywords: advanced encryption standard, photonic emission analysis attack, cryptographic chip, Hamming weight

PACS: 89.20.Ff, 85.60.–q, 07.05.Kf, 03.67.Dd **DOI:** 10.7498/aps.65.118901

* Project supported by the National Natural Science Foundation of China (Grant Nos. 51377170, 11304007), and the Natural Science Foundation of Hebei Province, China (Grant No. F2012506008).

† Corresponding author. E-mail: whswzx@aliyun.com