北京大学学报(自然科学版), 第 50 卷, 第 4 期, 2014 年 7 月
Acta Scientiarum Naturalium Universitatis Pekinensis, Vol. 50, No. 4 (July 2014)
doi: 10.13209/j.0479-8023.2014.096

针对 FPGA 实现的 AES 密码芯片的相关性电磁分析攻击

张潇　崔小欣†　魏为　黄颖　廖凯　廖楠　于敦山

北京大学信息科学技术学院微电子学研究院, 北京 100871; † 通信作者, E-mail: cuixx@pku.edu.cn

摘要　通过研究相关性电磁分析(CEMA)攻击方法, 构建电磁泄漏信息采集和数据处理平台, 对基于现场可编程门阵列(FPGA)实现的AES-128密码算法进行近场相关性电磁分析攻击。攻击结果表明, 该平台能够获取密码芯片工作时的电磁泄漏信息, 并通过分析获取 AES 第 10 轮加密的全部 16 个字节密钥。经过优化数据处理, 相关性电磁分析攻击的效率得到很大提高, 攻击所需的数据组数大大下降。

关键词　高级加密标准(AES); 可编程逻辑门阵列; 相关性电磁分析; 电磁信息泄漏

中图分类号　TN47

Correlation Electromagnetic Analysis Attacks against an FPGA Implementation of AES

ZHANG Xiao, CUI Xiaoxin†, WEI Wei, HUANG Ying, LIAO Kai, LIAO Nan, YU Dunshan

Institute of Microelectronics, School of Electronics Engineering and Computer Science, Peking University, Beijing 100871;
† Corresponding author, E-mail: cuixx@pku.edu.cn

Abstract　To study the vulnerability of Advanced Encryption Standard (AES) against electromagnetic side channel attacks, based on the method of correlation electromagnetic analysis (CEMA) attack, the authors built a platform to acquire EM emanation and process data, then performed a near-field CEMA attack against an FPGA implementation of AES-128. The results indicate that the platform is able to acquire the EM emanation of the encryption chip, and can retrieve all the 16 bytes of the 10th roundkey of AES. After the optimization of processing data, the efficiency of CEMA is highly enhanced, namely the data needed to exploit the correct roundkey is greatly reduced.

Key words　AES; FPGA; CEMA; EM emanation

2001 年 11 月, 美国国家标准和技术研究所(NIST)宣布 Rijndeal 算法成为新的数据加密标准——高级数据加密标准(AES)[1]。AES 的密码分析是当前密码学界比较关注的问题。传统的密码分析从密码算法的数学结构角度入手, 利用数学手段考虑密码算法的安全性, 通过大量数学计算搜寻密钥, 攻击难度很大。随后, 人们逐渐注意到, 在各种密码设备执行密码运算时会不可避免地泄露一些物理信息, 通过观测和分析这些泄露信息, 可以获取密码芯片中的敏感数据或密钥。利用算法硬件实现中的漏洞, 通过分析密码算法在运行过程中泄漏信息, 可以得到密钥的技术称为旁路攻击或侧信道攻击(side channel attack, SCA)。侧信道攻击具有很强的攻击能力, 自 1999 年 Kocher 等[2]成功用于攻击 DES 后, 引起业内人士的广泛关注。

根据泄漏信息的种类, SCA 可分为时间攻击[3]、能量分析攻击[4]和电磁分析攻击[5]等。功耗分析攻击较早受到重视, 但其实电磁泄漏相比能量消耗泄漏的信息更加丰富, 且电磁分析攻击时无需分解设备或改动电路, 故电磁分析攻击具有更强的实用性。

收稿日期: 2013–04–05; 修回日期: 2014–03–17; 网络出版日期: 2014–07–13

本文针对 FPGA 实现的 AES 密码系统, 采集其工作产生的电磁泄漏信号, 使用相关性分析的方法, 成功获取 AES 的轮密钥。

1 CEMA 攻击的一般步骤

相关性电磁分析(correlation electromagnetic analysis, CEMA) 攻击利用密码芯片电磁泄漏的数据依赖性, 其核心思想是: 通过模型模拟计算得到某一时刻的假设电磁泄漏值, 这一值与实际密码芯片在相应时刻处理对应中间值的电磁泄漏有较高的相关性。

CEMA 攻击可以归结为以下 5 个步骤[6]。

第 1 步 选择所执行算法(本文中为 AES)的某个中间值。这个中间值必须是一个函数 $f(d, k)$, 其中 d 一般是明文或者密文, k 是密钥的一部分(一般是某一字节), f 是加密算法的某一个或几个连续操作对应的函数。

第 2 步 测量电磁泄漏。对于 D 次加密或者解密, 攻击者首先要知道相应的数值 d, 以便用于第 1 步中对中间值的计算。将这些已知的数值记做向量 $\boldsymbol{d}=(d_1,\cdots,d_D)'$, 其中 d_i 表示第 i 次加解密对应的数据值(明文或密文)。

在每一次加密或解密期间, 攻击者都会记录一条电磁泄漏迹。将对应于数据 d_i 的能量迹记做 $\underset{t_i}{\rightarrow}'=(t_{i,1}, \ldots, t_{i,T})$。其中, T 表示该电磁迹的长度(采样点数)。对于 D 次操作, 会得到一个 $D\times T$ 大小的矩阵 $\boldsymbol{T}$ 表示 D 条电磁泄漏迹。

第 3 步 计算假设中间值。攻击的下一步是对于每个可能的 k 值, 计算其对应的假设中间值(hypothetical intermediate value), 将这些可能的值记为 $\boldsymbol{k}=(k_1, \ldots, k_K)$, 称为密钥假设(key hypotheses)。给定数据向量 $\boldsymbol{d}$ 和密钥假设 $\boldsymbol{k}$, 对于所有 D 次操作和所有 K 个密钥假设, 攻击者可以计算出假设中间值 $f(d, k)$, 并得到 $D\times K$ 大小的中间值矩阵 $\boldsymbol{V}$。

第 4 步 将中间值映射为电磁泄漏值。这里的电磁泄漏值为假设的电磁泄漏值。攻击者选定某一种模型, 将假设中间值矩阵 $\boldsymbol{V}$ 映射为假设电磁泄漏值矩阵 $\boldsymbol{H}$。

第 5 步 比较假设电磁泄漏值和第 2 步中采集到的电磁泄漏迹。将 $\boldsymbol{H}$ 的每一列(共 K 列)和 $\boldsymbol{T}$ 的每一列(共 T 列)进行比较, 做相关性分析, 得到 $K\times T$ 大小的相关性矩阵 $\boldsymbol{R}$, 其元素 r_{ij} 表示列 $\boldsymbol{h}_I$ 和 $\boldsymbol{t}_J$ 的相关程度。相关系数由下式计算:

$$r_{i,j}=\frac{\sum_{d=1}^{D}(h_{d,i}-\bar{h}_I)(t_{d,j}-\bar{t}_J)}{\sqrt{\sum_{d=1}^{D}(h_{d,i}-\bar{h}_I)^2\cdot\sum_{d=1}^{D}(t_{d,i}-\bar{t}_J)^2}}$$

其中, $\bar{h}_I$ 和 $\bar{t}_J$ 表示列 $\boldsymbol{h}_I$ 和 $\boldsymbol{t}_J$ 的均值。$r_{i,j}$ 越大, 列 $\boldsymbol{h}_I$ 和 $\boldsymbol{t}_J$ 的匹配程度越高。只要找到矩阵 $\boldsymbol{R}$ 中的最大元素 $r_{\mathrm{ck,ct}}$, 就可以得到正确的密钥索引 ck 以及处理相应中间值的时间点 ct。

2 汉明距离模型

目前, 攻击中一种常用的模型是汉明距离模型(Hamming distance model, HD model)[7]。两个二进制数 B_1 和 B_2 的汉明距离是它们异或值的汉明重量, 即 $\mathrm{HD}(B_1,B_2)=\mathrm{HW}(B_1\oplus B_2)$, 其中 HW 表示汉明重量, 是二进制数中 1 的个数。使用汉明距离模型基于以下两点假设: 1)电路中所有的 0→1 转换和 1→0 转换均会导致相同的电磁泄漏; 2)所有的 0→0 转换和 1→1 转换不会引起电磁泄漏。使用汉明距离模型的基本思想是计算 CMOS 数字电路在某个时间段内 0→1 转换和 1→0 转换的总数, 并以此刻画电路在该时段内的电磁泄漏。汉明距离模型可以较好地模拟 FPGA 实现的数字电路的寄存器的电磁泄露值。

3 对 AES 的 CEMA 攻击

本节介绍对 FPGA 实现的 AES 密码芯片的相关性电磁攻击的具体细节。攻击前, 首先在 PC 上生成待加密明文组成的文件, 并将 FPGA 密码芯片、电磁探头、示波器、PC、电源等试验设备进行连接, 如图 1 所示。探头紧贴芯片, 放置在芯片

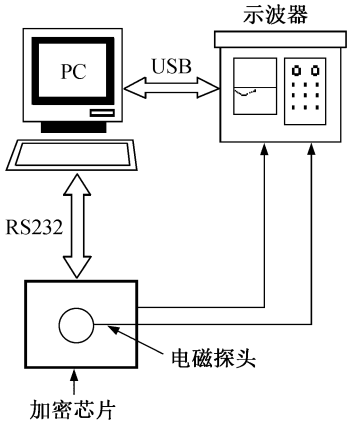


图 1 实验平台示意图
Fig. 1 Test platform sketch

上方, 如图 2 所示。AES 的密钥是已知的(为 3141592653589793238462643383279 5), 以便确认攻击结果。

之后 PC 向密码芯片发送明文, 密码芯片对接收到的明文进行加密, 同时示波器对电磁探头采集到的电磁泄漏信号进行采样。对所有明文加密结束后, 密码芯片和示波器分别把密文和电磁泄漏采样结果发送回到 PC, 可以得到攻击所需的所有的数据: 明文、密文和电磁泄漏值。

进行攻击前, 首先需要选定 AES 的一个中间值。由于在 FPGA 中, 加密时每个时钟周期进行一轮加密, 并对相关中间结果进行寄存, 这导致中间值只能选在各加密轮中间。考虑到 AES 的第 10 轮加密较为简单, 我们将中间值选定为第 9 轮的输出, 即第 10 轮的输入, 如图 3 所示。

我们选取汉明距离模型进行攻击。根据之前选定的中间值, 通过计算第 9 轮加密结果与第 10 轮加密结果(即密文)的汉明距离, 来描述最后一轮加密的电磁泄漏值, 即第 10 轮加密的电磁泄露值 $h_{i,j}=\mathrm{HD}(v_{i,j},\ d_i)=\mathrm{HW}(v_{i,j}\oplus d_i)$。其中, $v_{i,j}$ 为选定的中间值的某一个字节, d_i 为对应的密文字节。为了减少对应的密钥猜测数(2^8=256 种), 这里只选择一字节进行攻击。如果选择全部 16 字节进行攻击, 那么密钥猜测数为 2^{128} 种, 几乎无法进行攻击。

依次执行第 1 节中 CMEA 攻击的步骤, 可以得到最后的相关系数矩阵 ***R***。只要找到相关系数矩阵 ***R*** 的最大元素 $r_{\mathrm{ck,ct}}$, 其横坐标 ck 就是对应的密钥字节。之后, 依次选取中间值的不同字节进行攻击, 即可得到对应的不同字节的密钥, 从而恢复出整个

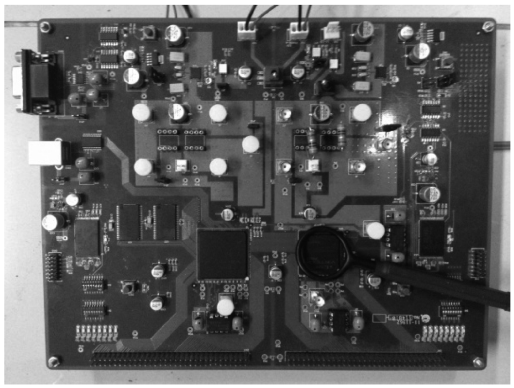


图 2　探头放置
Fig. 2　Position of probe

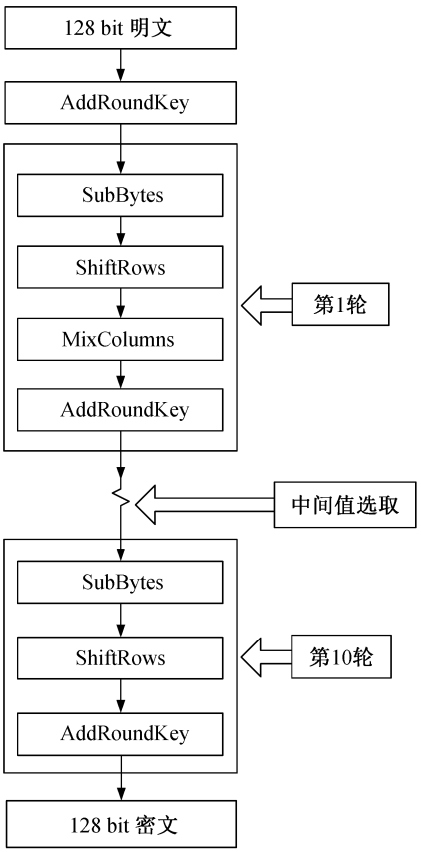


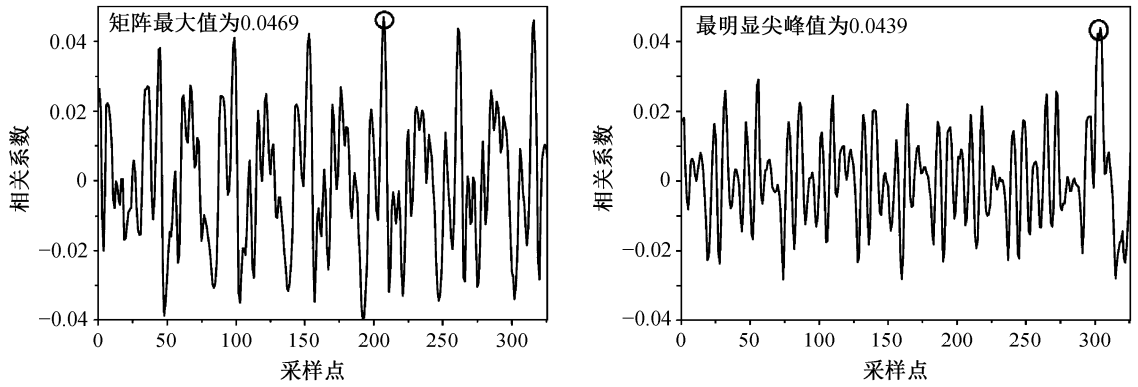
图 3　中间值选择
Fig. 3　Choosing intermediate value

轮密钥。最终, 可以成功获取 AES 第 10 轮的轮密钥 3FF86D98C44CCD429AF9F14CEAE 7538D。

4　对结果的分析和改进

首先引入一种对 ***R*** 矩阵可视化处理的方法: 在不同的图中显示该矩阵中的每一行, 如图 4 所示。这种情况下, 每个图对应一个密钥假设。图 4 中, 横坐标代表采样点数, 相当于加密时间, 纵坐标为相关系数。通过观察可以发现, 正确密钥假设对应的图中会出现明显的尖峰。

通过对加密结果进行分析, 我们可以得到: 1)随着攻击使用的电磁泄漏迹的增多, ***R*** 矩阵中的相关系数整体在下降, 但是正确密钥假设所在行的尖峰更加明显; 2)在攻击某些字节密钥时, 如果使用的电磁泄漏迹数量较少, 那么 ***R*** 矩阵中的最大元素 $r_{\mathrm{ck,ct}}$ 的横坐标 ck 并非正确的密钥字节; 但此时对 ***R*** 矩阵可视化处理后, 尖峰最明显的行对应的密钥假设却是正确的密钥字节。我们以对密钥第 8 字节的



(a) 密钥猜测为114 (b) 密钥猜测为66

图 4 最大值与最明显尖峰

Fig. 4 Max element vs. the most obvious peak

攻击为例(如图 4 所示), 使用 8000 组电磁迹时, 得到 $\boldsymbol{R}$ 矩阵的最大元素为 $r_{114,206}$, 但其横坐标 114 并非正确密钥字节, 正确字节而是 66。与此同时, 我们也在 $\boldsymbol{R}$ 矩阵第 66 行对应的图中观测到一个明显的尖峰, 而第 114 行对应的图则较为杂乱。

基于以上事实, 以 $\boldsymbol{R}$ 矩阵最大元素的横坐标为正确密钥字节显然不合适, 所以我们改进对 $\boldsymbol{R}$ 矩阵的处理: 以 $\boldsymbol{R}$ 矩阵中尖峰最明显的行的索引作为正确的密钥假设。结果表明, 比以 $\boldsymbol{R}$ 矩阵最大元素的横坐标作为正确密钥假设高效很多, 使攻击所需的电磁迹大大减少。

图 5 为电磁迹的数量与从中得到密钥的正确字节数的关系。其中, 实心方块曲线表示通过 $\boldsymbol{R}$ 矩阵中最大值的坐标确定密钥字节的方法(方法 1), 实心三角曲线是通过寻找 $\boldsymbol{R}$ 矩阵各行对应图中是否存在明显尖峰, 来确定密钥字节的方法(方法 2)。可以看出, 方法 2 更加高效。事实上, 使用方法 2 仅需 7552 条电磁迹即可恢复出全部密钥, 而此时通过方法 1 只能得到 13 个正确字节。而且, 实验结果表明, 即便增加到 32000 条电磁迹, 通过方法 1 也只得到 15 个正确字节, 而且增加过程中, 正确率有时甚至会下降; 对于方法 2, 只要电磁迹数大于 7552, 就一定可以得到全部 16 字节正确密钥。可以看出, 改进处理方法后, 大大降低了攻击所需的电磁迹的量。

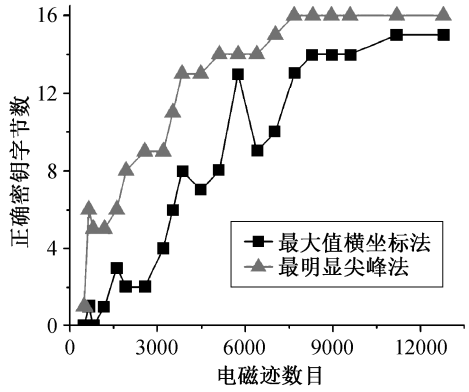


图 5 获得的正确密钥字节数

Fig. 5 Number of correctly extracted key bytes

本文攻击使用的电磁迹数量与其他方法[6,8]的对比如表 1 所示, 它们均是对 FGPA 实现的 AES 近场 CEMA 攻击。文献 [8] 中对 Kintex-7 XC7K325T 实现的 AES 进行 CEMA 攻击, 只需要使用 6000 条电磁迹, 这是得益于其使用的 FPGA 芯片采用了先进的 28 nm 工艺, 噪声更小, 而且在采集电磁泄漏时使用放大器和滤波器, 因此攻击效果很好。除此以外, 本文攻击所需的电磁迹数量是最少的, 说明本文的攻击效率较高, 对数据分析的改进成效显著。

表 1 与其他方法的对比

Table 1 Comparison to other methods

方法	FPGA	模型	电磁迹数目
本文	Virtex-2pro XC2VP7	HD	7556
文献[6]	–	HW	20000
文献[8]	Virtex-5 LX30/LX50	HD	19000
文献[8]	Kintex-7 XC7K325T	HD	6000

5 结论

本文针对 FPGA 实现的 AES 密码芯片进行近

场 CEMA 攻击, 构建采集电磁泄露信息的平台, 并根据 CEMA 攻击的一般步骤, 选取合适的攻击模型和中间值, 成功获取对应的第 10 轮的轮密钥。通过对数据处理方法的改进, 大大提高了攻击效率, 在使用 7552 组电磁泄漏迹及对应密文的情形下, 即可正确获取 AES 第 10 轮全部 16 字节密钥。CEMA 攻击不需要入侵密码芯片或者增加外围电路, 甚至可以不需要与芯片直接接触, 即可获取密码芯片的密钥等重要信息, 对密码芯片的安全构成严重威胁。因此, 在设计和使用密码芯片时, 需要增加对电磁分析攻击的防护措施, 这也是我们下一步工作的重点。

参考文献

[1] Daemen J, Rijmen V. The design of Rijndael: AES-the advanced encryption standard. Berlin: Springer, 2002

[2] Kocher P, Jaffe J, Jun B. Differential power analysis //Advances in Cryptology—CRYPTO'99. Berlin: Springer, 1999: 388–397

[3] Kocher P. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems // Advances in Cryptology — CRYPTO'96. Berlin: Springer, 1996: 104–113

[4] 刘上力. 高级数据加密标准的功耗分析及防范方法研究. 长沙: 中南大学, 2007

[5] Gandolfi K, Mourtel C, Olivier F. Electromagnetic analysis: Concrete results // Cryptographic Hardware and Embedded Systems—CHES 2001. Berlin: Springer, 2001: 251–261

[6] 段二朋, 严迎建, 李佩之. 针对 AES 密码算法 FPGA 实现的 CEMA 攻击. 计算机工程与设计, 2012, 33(8): 2926–2930

[7] Brier E, Clavier C, Olivier F. Correlation power analysis with a leakage model // Cryptographic Hardware and Embedded Systems-CHES 2004. Berlin: Springer, 2004: 16–29

[8] Hori Y, Katashita T, Sasaki A, et al. SASEBO-GIII: A hardware security evaluation board equipped with a 28-nm FPGA // Consumer Electronics (GCCE), 2012 IEEE 1st Global Conference on. Tsukub: IEEE, 2012: 657–660