doi:10.11959/j.issn.1000-436x.2016251

针对 AES 密码算法的多点联合能量分析攻击

杜之波[1]，孙元华[2]，王燚[1]
（1.成都信息工程大学信息安全工程学院，四川 成都 610225; 2.内江师范学院计算机科学学院，四川 内江 641100）

摘 要：针对 AES 密码算法的单个信息泄露点能量分析攻击，传统攻击方法没有尽可能多地利用算法和能量曲线中对攻击有用的信息，导致这种攻击存在所需曲线条数多、攻击信息利用率低等诸多问题。提出一种针对 AES 密码算法的多点联合能量分析攻击方法，并以相关性能量分析攻击为例，给出详细的攻击过程。攻击的同时选择轮密钥加和字节变换作为能量分析攻击的中间变量，构建关于该变量的联合能量泄露函数，实施多点联合的相关性能量分析攻击。针对智能卡上软实现的 AES 密码算法，分别进行联合能量分析攻击，针对轮密钥加和字节变换单个信息泄露点的相关性能量分析攻击实验，实验结果不仅验证了本攻击方法的有效性，而且证实联合能量分析攻击相比针对单个信息泄露点的能量分析攻击具有成功率高、所需攻击曲线条数少等优点。

关键词：多点联合能量分析攻击；相关性能量分析攻击；AES 密码算法；轮密钥加；字节变换
中图分类号：TP309.1 **文献标识码**：A

Multi-point joint power analysis attack against AES

DU Zhi-bo[1], SUN Yuan-hua[2], WANG Yi[1]
(1. College of Information Security Engineering, Chengdu University of Information Technology, Chengdu 610225, China;
2. School of Computer Science, Neijiang Normal University, Neijiang 641100, China)

Abstract: For the power analysis attack of the AES cryptographic algorithm with the single information leakage point, the traditional attack method does not use as much information as possible in the algorithm and power trace. So there are some problems such as required more power traces , the low utilization rate of information and so on. A novel method of muti-point joint power analysis attack against AES was proposed to solve the problems. And taking the correlation power analysis attack as an example, the detailed attack process was presented. The operations of the round key addition and the SubBytes were chosen as the attack intermediate variable at the same time. Then the joint power leakage function was constructed for the attack intermediate variable. And the multi-point joint correlation energy analysis attack was given. Aiming at the AES cryptographic algorithm implemented on the smart card, the multi-point joint power analysis attack, the correlation power analysis attack with the single information leakage point in the key addition and the SubBytes were conducted. The measured results validate the proposed method is effective. It also shows that the proposed method has the advantages of high success rate and less power traces comparing with the single information leakage point.

Key words: multi-point joint power analysis attack, correlation power analysis attack, AES cryptographic algorithm, round key addition, SubBytes

收稿日期：2016-09-15
基金项目：“核高基”国家科技重大专项基金资助项目(No.2014ZX01032401-001)；国家高技术研究发展计划（“863”计划）基金资助项目(No.2012AA01A403) ；四川省科技支撑计划项目基金资助项目(No.2014GZ0148)；四川省教育厅重点科研基金资助项目(No.13ZA0091)；成都信息工程大学科研人才基金资助(No.XAKYXM008)
Foundation Items: The National Science and Technology Major Project of Hegaoji (No.2014ZX01032401), The National High Technology Research and Development Program (863 Program) (No.2012AA01A403), The Key Technology Research and Development Program of Sichuan Province (No.2014GZ0148), The Major Scientific Research Foundation of Sichuan Educational Commission (No.13ZA0091), The Scientific Research Talent Fund of CUIT(No.XAKYXM008)

1　引言

随着网络空间安全技术的发展，作为网络空间安全理论基础的密码学，其安全性成为网络空间安全研究的方向之一。密码学的安全包括密码算法的安全和密码算法实现的安全，传统密码分析学主要从数学分析方法上研究和证明密码算法的安全。密码算法的安全，并不意味着密码算法实现的安全。密码算法的实现，终究脱离不了运行的载体，无论软实现的密码算法还是硬实现的密码算法，自能量分析攻击[1]（power analysis attack）技术被首次提出，研究者在关注密码算法安全的同时，开始研究密码电子设备等密码算法实现的安全。于是出现了针对密码算法的能量分析攻击[2]、电磁分析攻击[3]、故障注入分析攻击[4]和代数侧信道攻击[5]等侧信道攻击技术。其中，能量分析攻击，利用密码电子设备运行时泄露的能量信号物理特征，结合信号分析和统计学等技术来破解密钥。因所需测量设备简单、易实施，能量分析攻击成为侧信道攻击常用的攻击方法之一。

在侧信道攻击中，针对分组密码算法的侧信道攻击是常见的攻击研究对象，包括 DES 密码算法[2,6]、高级加密标准[7~15]（AES，advanced encryption standard）算法和 SM4 密码算法[16,17]等。AES 是是 1997 年美国 ANSI 向全球发起征集加密算法作为数据加密标准，最终 Rijndael 算法入选，成为商用密码领域应用最广泛的对称密码算法之一。目前针对 AES 密码算法的侧信道能量分析攻击的研究，主要从攻击和防御这 2 个方面展开，文献[7~10]实现了针对 AES 密码算法的简单能量分析攻击、差分能量分析攻击、二阶差分能量分析攻击和频域的相关性能量分析攻击。文献[11,12]设计和实现了 AES 密码算法防御侧信道攻击的防御方案。针对 AES 密码算法侧信道攻击的研究还包括了 Cache 攻击[13]、毛刺攻击[14]和碰撞攻击[15]等多种侧信道攻击方法。多点联合能量分析攻击[18]可以提高能量曲线中信息利用率，降低能量分析攻击的曲线条数等。目前，在国内外公开发表的文献中针对 AES 密码算法各个攻击点之间相关性的研究，以及联合 AES 密码算法各个攻击点进行侧信道能量分析攻击，尚未发现有相关的成果。本文以 AES 密码算法为攻击对象，提出了针对 AES 密码算法轮密钥加和字节变换的多点联合能量分析攻击，并给出了详细的攻击过程。对 AES 智能卡进行了实际攻击测试，攻击结果通过针对 AES 密码算法轮密钥加的相关性能量分析攻击和针对 AES 密码算法字节变换输出的相关性能量分析攻击对比，验证本攻击方法的有效性和优劣。

本文对 AES 密码算法攻击对象进行概述；介绍相关性能量分析攻击原理和攻击过程；详述了 AES 密码算法的信息泄露和攻击点，并给出了每个信息泄露点对应的泄露函数；介绍了针对 AES 密码算法轮密钥加和字节变换的多点联合能量分析攻击方法，通过构建 AES 密码算法轮密钥加和字节变换的联合泄露函数，设计和提出针对 AES 密码算法轮密钥加和字节变换的多点联合能量分析攻击方法，并给出了详细的攻击过程；对智能卡上软实现的 AES 密码算法行了多点联合相关性能量分析攻击测试，实验结果不仅验证了攻击方法的有效性，而且验证了相比于针对单个信息泄露点的相关性能量分析攻击，该攻击方法可以降低能量分析攻击所需曲线条数，提高成功率。

2　攻击算法描述

高级加密标准算法 AES 密码算法是采用 square 结构、长度为 128 bit 的分组密码算法，密钥长度为 128 bit、192 bit 或 256 bit，相应的迭代轮数分别为 10 轮、12 轮和 14 轮，轮结构的变换主要有 4 种基本变换组成：字节变换(SubBytes)、行移位(shift rows)、列混合(mix columns)和轮密钥加(add round keys)，以加密算法为例，128 bit 的 AES 密码算法的运算流程如图 1 所示。

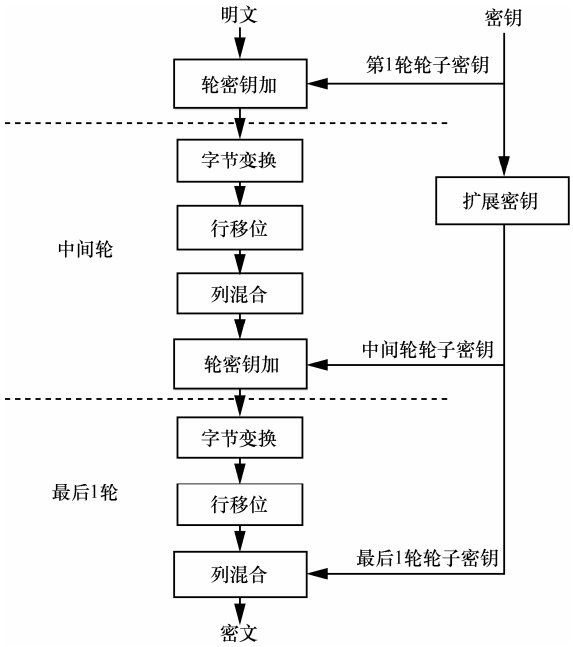


图 1　AES 密码算法的运算流程

字节变换是基于 S 盒的非线性变换，字节变换有 16 个相同 S 盒构成，每个 S 盒为 8 进 8 出，表示为 $b_{i,r}$=*SubByte*($a_{i,r}$)，用 $b_{i,r}$ 、 $a_{i,r}$ 表示中间状态，其中，$a_{i,r}, b_{i,r} \in Z_2^8$，$i,r$ 表示行号和列号，$i,r \in [0,3]$。

行移位是在 AES 密码算法中间状态不同行上进行循环移位操作，详细的运算过程如图 2 所示。

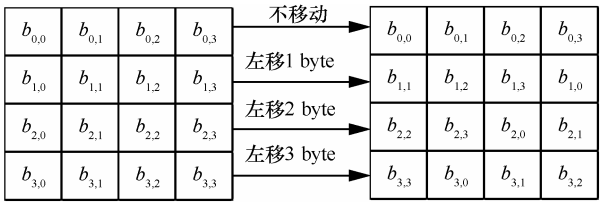


图 2　AES 行移位变换

列混合通过有限域上 GF(2^8)的矩阵相乘来实现，如式(1)所示，其中，$c_{i,r} \in Z_2^8$。

$$\begin{bmatrix} c_{0,r} \\ c_{1,r} \\ c_{2,r} \\ c_{3,r} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} b_{0,r} \\ b_{1,r} \\ b_{2,r} \\ b_{3,r} \end{bmatrix} \tag{1}$$

轮密钥加是 AES 密码算法的中间状态数据 $c_{i,r}$ 与子密钥 $k_{i,r}$ 进行异或运算。

3　能量分析攻击原理

侧信道能量分析攻击包括相关性能量分析攻击[19, 20](CPA，correlation power analysis attack)、差分能量分析攻击、简单能量分析攻击和模板攻击，其中，相关性能量分析攻击是通过计算被攻击中间变量的假设能耗值和真实能量信号之间的相关系数来破解密钥，其详细的攻击过程如下所示。

1) 采集密码电子设备在进行加密、解密、签名等运算过程时运行的能量信号，不同时刻点上的能量信号构成能量信号曲线，表示为 T，采集的曲线条数为 N。

2) 确定算法中和密钥相关的中间变量 V，猜测密钥，根据能量模型，构建关于该中间变量的泄露函数，计算假设能耗值。

3) 根据皮尔逊相关系数，计算假设能耗值和真实能量信号曲线之间的相关性，相关系数最大时对应的猜测密钥为要破解的密钥。

4　AES 密码算法的信息泄露点

根据侧信道相关性能量分析攻击原理，CPA 攻击的关键在于确定算法中和密钥相关的中间数据，以 AES 密码算法的第 1 轮为例，针对 AES 密码算法的潜在的攻击和信息泄露点为 pos_1、pos_2、pos_3 和 pos_4，如图 2 所示。

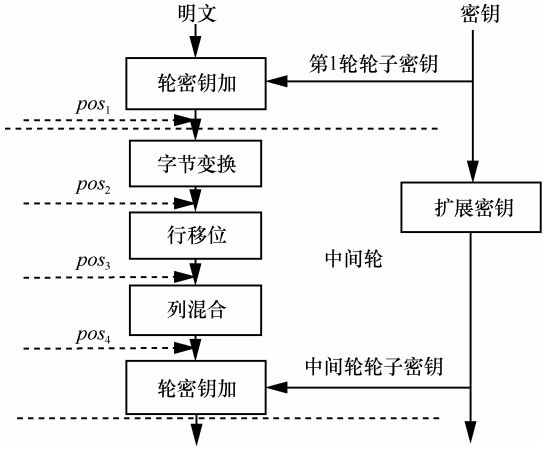


图 3　AES 算法信息泄露点

在图 3 中，pos_1 对应的攻击和信息泄露点为轮密钥加输出，相关性能量分析攻击的中间变量 $d_{i,r}$ 计算表达式如式(2)所示，攻击时以 $d_{i,r}$ 来构建泄露函数。

$$d_{i,r} = f(m_{i,r}, k_{i,r}) = m_{i,r} \oplus k_{i,r} \tag{2}$$

在图 3 中，pos_2 对应的攻击和信息泄露点为字节变换输出，相关性能量分析攻击的中间变量 $d_{i,r}$ 计算表达式如式(3)所示，攻击时以 $d_{i,r}$ 来构建泄露函数。

$$d_{i,r} = f(m_{i,r}, k_{i,r}) = SubByte(m_{i,r} \oplus k_{i,r}) \tag{3}$$

在图 3 中，pos_3 对应的攻击和信息泄露点为行移位输出，由于行移位只是改变字节变换输出字节位置，所以 pos_3 对应的攻击变量和 pos_2 相同。

在图 3 中，pos_4 对应的攻击和信息泄露点为列混合输出 $c_{i,r}$，由于 $c_{i,r}$ 的 1 个字节是由输入的 4 个字节通过有限域上乘法和异或运算计算所得，所以 $c_{i,r}$ 和轮子密钥的 4 个字节相关，如果直接选择 $c_{i,r}$ 进行攻击，则 CPA 的密钥空间为 $[0, 2^{32}-1]$，为了降低攻击时密钥搜索范围和计算复杂度，一般通过选择明文来实施，以攻击 $k_{0,0}$ 为例，通过选择明文，使 $b_{0,0}$ 为随机数据，$b_{1,0}$ 、$b_{2,0}$ 和 $b_{3,0}$ 为固定数据，根据中间变量 $d_{0,0}$ 来实施攻击，如式(4)所示。

$$d_{i,r} = f(b_{0,0}, b_{1,0}, b_{2,0}, b_{3,0}) = \left[02 \times b_{0,0}\right] \oplus \left[03 \times b_{1,0}\right] \oplus \left[01 \times b_{2,0}\right] \oplus \left[01 \times b_{3,0}\right] \tag{4}$$

5　针对 AES 密码算法的多点联合能量分析攻击算法

如果单独选择式(2)~式(4)进行能量分析攻击，则可以攻击出同一密钥 $k_{i,r}$，但是这种攻击方法并没有考虑 AES 密码算法各个信息泄露点之间的关联，以及各个信息泄露点和同一密钥存在相关性这一特性。实际 AES 密码算法电子产品在进行完整的加解密运算时，轮密钥加、字节变换和列混合会出现在一次完整的运算过程中，对应在采集的能量曲线上，式(2)、式(3)和式(4)对应不同时间点上的能量信号迹，加之三者和同一密钥存在相关性，所以如果单独选择一个信息泄露点进行能量分析攻击，那么这种攻击方式没有尽可能多地利用能量曲线中泄露的和攻击相关的有用信息，导致这种攻击的信息利用率和曲线利用率低。

由于 AES 信息泄露点对应的中间数据和同一密钥存在相关性，所以可以构造和多个信息泄露点相关的联合能量泄露函数，进行多点联合相关性能量分析攻击(MJPAA, multi-point joint power analysis attack)，通过均值能量曲线的距离平方和方法，确定式(2)和式(3)在能量曲线中对应的信息泄露点，结合相关性能量分析攻击原理，针对 AES 密码算法轮密钥加和字节变换的多点联合能量分析攻击方法如下所示。

1) 随机明文，采集被攻击 AES 密码设备运行加解密时的能量曲线 t_n，n 表示采集的第 n 条曲线，同时记录每条曲线对应的明文输入 M_n，每个明文以字节为基本单位转换为状态字节，表示为 $m_{i,r}$。

2) 同时选择 pos_1 和 pos_2 为攻击点，以式(2)和式(3)为基础，构建多点联合相关性能量分析攻击的中间变量。

3) 根据 $m_{i,r}$，将能量曲线 t_n 按值分类，分为不同的曲线集合，如式(5)所示。

$$T_\lambda = \{t_n \mid m_{i,r} = \lambda,\ \lambda \in [0,255]\} \tag{5}$$

4) 根据式(6)计算每个能量曲线集合的均值曲线

$$\overline{T_\lambda} = \frac{1}{|T_\lambda|}\sum_{t_n \in T_\lambda} t_n \tag{6}$$

其中，$|T_\lambda|$ 表示能量曲线集合 T_λ 中曲线条数。

5) 根据式(7)计算不同集合的均值能量曲线之间的距离平方和曲线 $sosd(\tau)$。

$$sosd(\tau) = \sum_{\alpha<\beta}\left(\overline{T_\alpha}(\tau) - \overline{T_\beta}(\tau)\right)^2 \tag{7}$$

6) 在距离平方和曲线 $sosd(\tau)$ 中，确定幅值最大的 2 个点所对应的时刻点 μ 和 v，其中，$\mu < v$，μ 表示轮密钥的输出产生的能量信号，对应于攻击和信息泄露点 pos_1；时刻点 v 表示字节变换输出产生的能量信号，对应于攻击和信息泄露点 pos_2。

7) 分别以时刻点 μ 和 v 为中心，每条曲线前后取 l 个能量信号点，这样原始的能量曲线分成了 2 个能量曲线集合，表示为 T_μ 和 T_v，T_μ 表示以 μ 为中心截取的能量曲线集合，对应于信息泄露点 pos_1；T_v 表示以 v 为中心截取的能量曲线集合，对应于信息泄露点 pos_2。

8) 根据第 3 节攻击过程的步骤 2)，同时选择式(2)和式(3)的运算结果作为能量分析攻击的中间变量，根据变量的能量模型，构建轮密钥的输出和字节变换输出的多点联合的能量泄露函数 $UF(m_{i,r}, k_{i,r})$，其中，能量曲线的集合为 $\{T_\mu, T_v\}$，以汉明重量模型为例，构建的多点联合的能量泄露函数如式(8)所示。

$$UF(m_{i,r}, k_{i,r}) = \begin{cases} HW(m_{i,r} \oplus k_{i,r}), t_n \in T_\mu \\ HW(SubByte(m_{i,r} \oplus k_{i,r})), t_n \in T_v \end{cases} \tag{8}$$

9) 猜测 $k_{i,r}$，根据式(8)计算第 3 节攻击过程的步骤 2)所述的假设能耗值。

10) 根据皮尔逊相关系数，计算假设能耗值和真实能量信号曲线之间的相关性，其中，真实能量信号曲线集合为 $\{T_\mu, T_v\}$，系数最大时对应的密钥即为攻击出的密钥。

6　针对 AES 多点联合的相关性能量分析攻击实验

为验证攻击方法的有效性，实验对智能卡上软实现的 AES 密码算法进行了攻击测试。同时为了测试多点联合相关性能量分析攻击的性能，实验还对轮密钥加和字节变换输出进行了单点相关性能量分析攻击。实验环境为：智能卡 PA/EMA 采集仪 power detector、示波器、工作站和数据分析软件 Inspector。攻击实验采集的到能量曲线波形数据如图 4 所示，数据的采样频率为 250 MHz。

6.1　攻击过程

以攻击 $k_{0,0}$ 为例，选择图 4 中 AES 密码算法第 1 轮能量曲线的开始部分曲线，如图 5 所示。

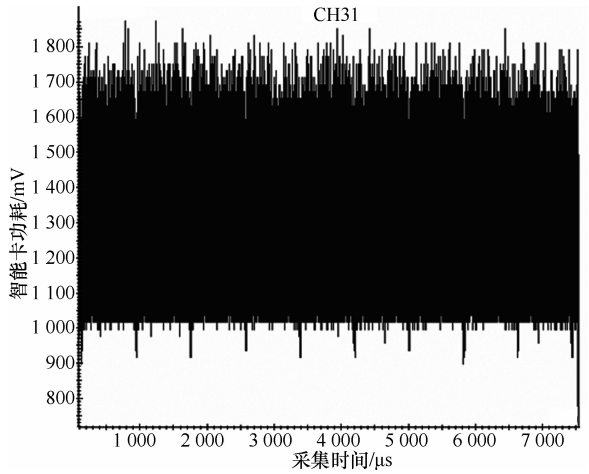


图 4　AES 密码算法功耗波形

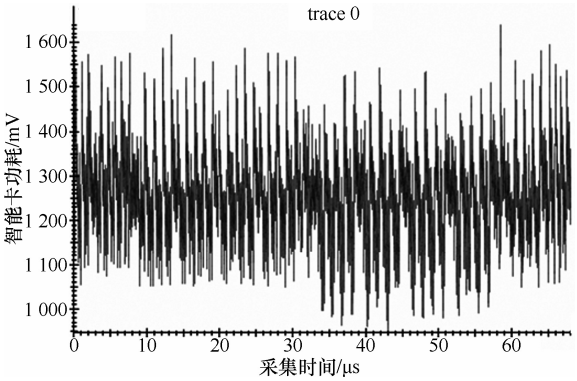


图 5　AES 密码算法第一轮开始部分曲线

根据第 5 节所述攻击过程的步骤 3)、步骤 4)和步骤 5)，计算距离平方和曲线 $sosd(\tau)$，计算结果如图 6 所示。

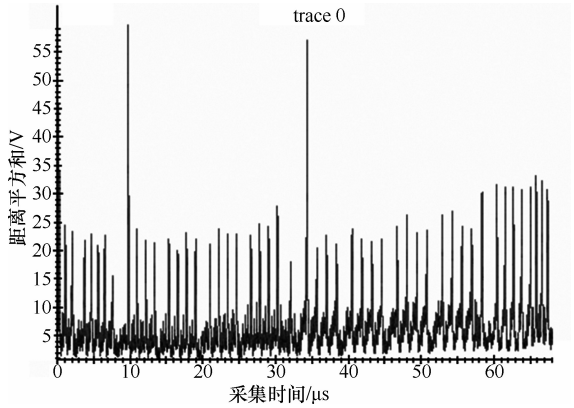


图 6　距离平方和曲线

根据第 5 节所述攻击过程的步骤 6)，在图 6 中确定尖峰幅值最大的 2 个点所对应的时刻点 μ=9.66 μs，v=34.26 μs。

根据第 5 节所述攻击过程的步骤 7)，分别以 μ 和 v 为中心，对每条能量曲线向前和向后取 20 个点，形成 2 个能量曲线集合 T_μ 和 T_v。

根据第 5 节所述攻击过程的步骤 8)、步骤 9)和步骤 10)进行多点联合的相关性能量分析攻击，攻击结果如图 7 所示。

```
analyzed key byte 0
best correlation:
0，key byte candidate：43(0x2B)，value：0.609 6，at position：12
1，key byte candidate：242(0xF2)，value：−0.542 2，at position：16
2，key byte candidate：144(0x90)，value：−0.531 2，at position：14
3，key byte candidate：152(0x98)，value：−0.521 4，at position：14
4，key byte candidate：214(0xD6)，value：−0.509 5，at position：13
5，key byte candidate：41(0x29)，value：0.505 3，at position：11
best key byte 0 data:0x2B
```

图 7　$k_{0,0}$ 攻击结果

同理可对 AES 密码算法的其他密钥字节进行攻击，最终的攻击结果为 0x2B7E151628AED2A6ABF7158809CF4F3C，将该密钥对智能卡加密的明文进行 AES 加密运算，所得密文和智能卡进行 AES 加密返回的密文相同，则验证了本攻击密钥的正确性，进一步也验证了多点联合相关性能量分析攻击方法的有效性。

6.2　攻击结果对比分析

为测试多点联合相关性能量分析攻击的攻击效率，攻击实验还分别对 pos_1 对应的轮密钥加和 pos_2 对应的字节变换输出进行了相关性能量分析攻击。针对 AES 密码算法轮密钥加和字节变换的多点联合能量分析攻击、针对 AES 密码算法轮密钥加的相关性能量分析攻击和针对 AES 密码算法字节变换输出的相关性能量分析攻击三者的实验攻击测试分别是 10 次，攻击结果如图 8 所示。

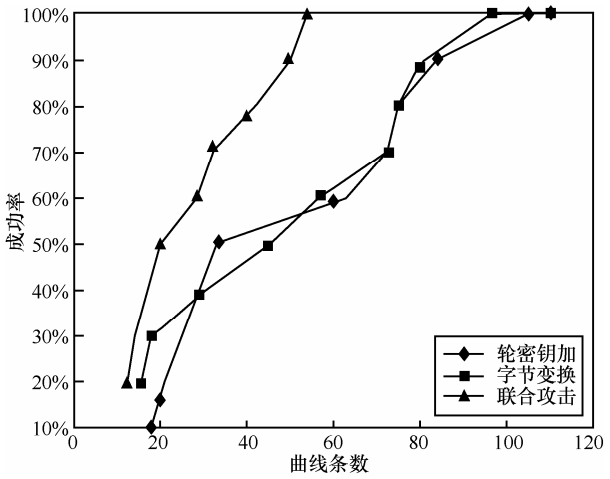


图 8　攻击实验对比

从图 8 可知，在相同成功率下，针对 AES 密码算法轮密钥加的相关性能量分析攻击和针对 AES 密码算法字节变换输出的相关性能量分析攻击所需能量曲线条数要多于针对 AES 密码算法轮密钥加和字节变换的多点联合能量分析攻击所需能量曲线条数，二者所需能量曲线条数近似于针对 AES 密码算法轮密钥加和字节变换的多点联合能量分析攻击所需能量曲线条数的 2 倍。

在相同的曲线条数下，针对 AES 密码算法轮密钥加和字节变换的联合相关性能量分析攻击的成功率，近似于针对 AES 密码算法单个信息泄露点相关性能量分析攻击成功率的 2 倍。

此外，从图 8 中还可以看出，在针对 AES 密码算法的联合能量分析攻击中，随着曲线条数的增加，成功率的增长速度要快于针对 AES 密码算法单个信息泄露点的相关性能量分析攻击。

总之，三者实验结果表明针对 AES 密码算法的轮密钥加和字节变换的联合相关性能量分析攻击通过利用 2 个信息点的泄露，提高了攻击的成功率，降低了攻击所需曲线条数，攻击效果要优于针对 AES 密码算法单个信息泄露点的相关性能量分析攻击。

7　结束语

本文对 AES 密码算法的信息泄露点和攻击点进行了详细分析，每个攻击点都可以进行相关性能量分析攻击，但是这种攻击方式并没有尽可能多地利用单次采集的能量曲线中和攻击相关的有用信息，导致能量曲线的利用率低。为此提出了针对 AES 密码算法轮密钥加和字节变换的多点联合能量分析攻击方法，该攻击方法同时构建轮密钥的输出和字节变换输出的多点联合的能量泄露函数，设计和实现了联合 2 个信息泄露点的相关性能量分析攻击。实验对针对 AES 密码算法轮密钥加和字节变换的多点联合能量分析攻击、针对 AES 密码算法轮密钥加的相关性能量分析攻击和针对 AES 密码算法字节变换输出的相关性能量分析攻击这 3 种攻击方式进行了测试对比，结果表明多点联合能量分析攻击在攻击的成功率和攻击所需曲线条数这 2 个指标上，都要优于针对单个信息泄露点的能量分析攻击。下一步研究将多点联合模型应用到其他密码算法的能量攻击和其他类型的能量分析攻击方法中。

参考文献：

[1] KOCHER P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[C]//Advances in Cryptology. 1996: 104-113.

[2] KOCHER P C, JAFFE J, JUN B. Differential power analysis[M]. Berlin: Springer, 1999:388-397.

[3] QUISQUATER J J. A new tool for non-intrusive analysis of smart cards based on electromagnetic emissions, the SEMA and DEMA methods[J]. Eurocrypt 2000 Rump Session, 2000.

[4] BONEH D, DEMILLO R A, LIPTON R J. On the importance of checking cryptographic protocols for faults[C]//International Conference on Theory & Application of Cryptographic Techniques. 1997: 37-51.

[5] STANDAERT F X, MALKIN T G, YUNG M. A unified framework for the analysis of side channel key recovery attacks[C]//28th Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2009: 443-461

[6] ABID T, ALI M. Differential power analysis countermeasure for improved DES with dynamic key management[J]. Bahria University Journal of Information & Communication Technology, 2015, 8(2):15-21.

[7] MANGARD S. A simple power-analysis (SPA) attack on implementations of the AES key expansion[C]//International Conference on Information Security and Cryptology. 2002: 343-358.

[8] ORS S B, GURKAYNAK F, OSWALD E, et al. Power-analysis attack on an ASIC AES implementation[C]//International Conference on Information Technology: Coding and Computing. 2004: 546-552.

[9] OSWALD E, MANGARD S, HERBST C, et al. Practical second-order DPA attacks for masked smart card implementations of block ciphers[C]//Cryptographers' Track at The RSA Conference. 2006: 192-207.

[10] 向春玲, 吴震, 饶金涛, 等. 针对一种 AES 掩码算法的频域相关性能量分析攻击[J]. 计算机工程, 2016, 42(10): 146-150.
XIANG C L, WU Z, RAO J T, et al. Correlation power analysis attack in frequency domain for an AES mask algorithm[J]. Computer Engineering, 2016, 42(10): 146-150.

[11] OSWALD E, MANGARD S, PRAMSTALLER N, et al. A side-channel analysis resistant description of the AES S-box[C]// International Workshop on Fast Software Encryption. 2005: 413-423.

[12] BONNECAZE A, LIARDET P, VENELLI A. AES side-channel countermeasure using random tower field constructions[J]. Designs, codes and Cryptography, 2013, 69(3): 331-349.

[13] OSVIK D A, SHAMIR A, TROMER E. Cache attacks and countermeasures: the case of AES[C]//Cryptographers' Track at the RSA Conference. 2006: 1-20.

[14] MANGARD S, SCHRAMM K. Pinpointing the side-channel leakage of masked AES hardware implementations[C]//International Workshop on Cryptographic Hardware and Embedded Systems.

2006: 76-90.

[15] MORADI A, MISCHKE O, EISENBARTH T. Correlation-enhanced power analysis collision attack[C]//International Workshop on Cryptographic Hardware and Embedded Systems. 2010: 125-139.

[16] 杜之波, 吴震, 王敏, 等. 针对 SM4 轮输出的改进型选择明文功耗分析攻击[J]. 通信学报, 2015, 36(10): 85-91.
DU Z B, WU Z, WANG M, et al. Improved chosen-plaintext power analysis attack against SM4 at the round-output[J]. Journal on Communications, 2015, 36(10): 85-91.

[17] 王敏, 杜之波, 吴震, 等. 针对 SMS4 轮输出的选择明文能量析攻击[J]. 通信学报, 2015, 36(1): 2015016.
WANG M, DU Z B, WU Z, et al. Chosen-plaintext power analysis attack against SMS4 with the round-output as the intermediate data[J]. Journal on Communications, 2015, 36(1): 2015016.

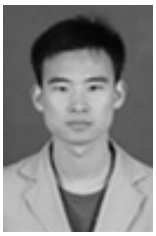
[18] 杜之波, 吴震, 王敏, 等. 针对 SM4 密码算法的多点联合能量分析攻击[J]. 计算机研究与发展, 2016, 53(10): 2224-2229.
DU Z B, WU Z, WANG M, et al. Multi-point joint power analysis attack against SM4[J]. Journal of Computer Research and Development, 2016, 53(10): 2224-2229.

[19] MANGARD S, OSWALD E, POPP T. Power analysis attacks: revealing the secrets of smart cards[M]. Berlin: Springer, 2008.

[20] 杜之波, 吴震, 王敏, 等. 针对基于 SM3 的 HMAC 的能量分析攻击方法[J]. 通信学报, 2016, 37(5): 38-43.
DU Z B, WU Z, WANG M, et al. Power analysis attack of HMAC based on SM3[J]. Journal on Communications, 2016, 37(5): 38-43.

作者简介：

杜之波（1982-），男，山东冠县人，成都信息工程大学讲师，主要研究方向为信息安全、侧信道攻击与防御、天线应用和物联网安全。



孙元华（1982-），男，山东冠县人，博士，内江师范学院讲师，主要研究方向为天线设计、信息安全和物联网安全。

王燚（1968-），男，四川成都人，博士，成都信息工程大学教授，主要研究方向为机器学习、侧信道攻击与防御、自然语言处理。