·安全技术· 文章编号:1000-3428(2017)10-0120-06 文献标志码:A 中图分类号:TP309

一种带掩码 AES 算法的高阶差分功耗分析攻击方案

段晓毅,王思翔,崔 琦,孙渴望

(北京电子科技学院 电子信息工程系,北京 100070)

摘 要: 鉴于能量分析攻击对密码芯片安全性的严重威胁,对掩码技术进行研究,提出一种通过使用预处理函数对固定值掩码进行攻击的高阶差分功耗分析(HODPA)方案。利用功耗曲线上 2 个信息点的联合分布绕过掩码对加密系统的保护。开发以 MEGA16 单片机为核心的侧信道攻击平台,并在该平台上进行实验验证,结果表明,在不明确掩码具体数值的情况下,一阶 DPA 无法恢复出正确密钥,HODPA 方案仅需约 500 条功耗曲线即可得到正确密钥,且正误密钥之间区分度高,具有较强的实用性。

关键词: 掩码技术;预处理函数;差分功耗分析;功耗曲线;AES 算法

中文引用格式: 段晓毅,王思翔,崔 琦,等. 一种带掩码 AES 算法的高阶差分功耗分析攻击方案[J]. 计算机工程,2017,43(10):120-125.

英文引用格式: DUAN Xiaoyi, WANG Sixiang, CUI Qi, et al. A High-order Differential Power Analysis Attack Scheme with Masked AES Algorithm[J]. Computer Engineering, 2017, 43(10): 120-125.

A High-order Differential Power Analysis Attack Scheme with Masked AES Algorithm

DUAN Xiaoyi, WANG Sixiang, CUI Qi, SUN Kewang

(Department of Electronics and Information Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China)

【Abstract】 In view of the serious threats that power analysis attacks causes on the security of the cipher chip, based on the in-depth study of masked technology, this paper proposes a High Order Differential Power Analysis(HODPA) scheme which attacks the fixed value mask through the use of preprocessing function. By using the joint distribution of the two points on the power curve, this method successfully bypasses the mask's protection of the system. It develops a side channel attack platform based on MEGA16 and carries out the experimental verification. Experimental result shows that, without knowing the specific masked value, the ordinary first order DPA cannot recover the correct key, but HODPA only needs about 500 power curves to get the correct key, and discrimination between correct key and wrong keys is high, fully proves the validity and practicability of the scheme.

【Key words】 masked technology; preprocessing function; Differential Power Analysis(DPA); power curve; AES algorithm

DOI: 10.3969/j.issn.1000-3428.2017.10.021

0 概述

侧信道攻击是一种通过利用芯片泄漏的物理信息并对其进行统计分析以获得芯片内部的敏感信息[1]的一种攻击方法。而作为目前应用最为广泛的侧信道分析攻击技术,差分功耗分析(DPA)因为其具有攻击工具易于获取、适应性强等特点,对密码芯片的现实安全造成了严重威胁。

为抵抗此类攻击,文献[2]于 1999 年提出对算法进行掩码操作的方法,之后文献[3]从理论上证明了该方法对一阶 DPA 的良好抗性,文献[4]通过对运行在智能卡上的 AES 添加掩码并实施 DPA 攻击证明了该方法的有效性。随着研究的深入,文献[5]于 2000 年从实现上给出了针对带掩码保护的密码算法的攻击思路,文中指出,如果密码设备泄漏了汉明重量信息,那么在使用绝对差值函数对功耗曲线进行预处理之后,进行高阶差分功耗分析(HODPA)攻击可以取得较好的效果。但是文献[5]本身也存在不少问题,首先没有从理论上证明其给出的预处理函数一定能够产生最好的攻击效果,其次也没有说明如何确定功耗曲线中需要进行相减操作的 2 个点的位置。2003 年,文献[6]提

基金项目: 北京市自然科学基金(4163076,4152048);北京电子科技学院基金(328201505,328201508)。

作者简介: 段晓毅(1979—),男,讲师、博士,主研方向为密码学、计算机检测技术;王思翔、崔 琦、孙渴望,硕士研究生。

收稿日期: 2016-08-18 **修回日期:** 2016-10-09 **E-mail:** 691213491@qq.com

出如果攻击加密算法运行的第一轮和最后一轮,并假设这些轮中使用了相同的掩码,那么相减的 2 个点将会出现在各轮中相同的位置,大大简化了实际攻击中 HODPA 的计算复杂度。

2005 年,文献[7]指出预处理对二阶 DPA 的攻击效果具有显著影响。他们研究了汉明重量模型和汉明距离模型中的绝对差值函数,证明了在 2 个模型中都可以使用该预处理函数。这个结论后来由文献[8]在一个实际攻击中进行了验证。此外还发现,如果把绝对差值函数与乘方函数相结合,相关性仅会得到小幅增加。文献[9]描述一个对分组密码实施的二阶 DPA 攻击策略。文献[10]使用该策略来分析分组密码 ARIA 的掩码型实现,他们在理论上证明了在第一轮和最后一轮加密中,不同中间结果的组合通常是很好的攻击目标。2014 年,文献[11]提出了一个对带掩码设备进行高阶 DPA 攻击的统计模型,进一步证明了高阶 DPA 是处理低信噪比功耗曲线的最佳选择。2015 年,文献[12]从理论上说明了攻击区间的选择对高阶 DPA 成功率的影响。

高阶 DPA 攻击就是对预处理之后的功耗曲线的 DPA 攻击,使用多个中间值构造出合适的联合中间值,并利用汉明重量模型或汉明距离模型将其映射为猜测的功耗消耗值。本文搭建一个基于带掩码密码芯片的侧信道功耗数据采集和分析平台,采集 mage16 密码芯片在加密处理过程中的功耗信息,并在这些工作的基础上,研究针对有掩码 AES 算法实施高阶 DPA 攻击的可能性。本文从理论和实践两方面说明高阶 DPA 技术对带有掩码保护的密码芯片进行侧信道攻击的优越性,提出一种通过使用预处理函数对固定值掩码进行攻击的高阶差分功耗分析方案。

1　带掩码加密算法的高阶 DPA 攻击

1.1　掩码技术

掩码技术是一种得到了学术界广泛关注和认可的侧信道攻击防御对策,之所以有很多密码芯片的设计方案会使用掩码技术来抵抗功耗分析攻击,其原因是多方面的。其中最重要的一点就是掩码技术可以在无须改变处理器功耗消耗特征的情况下,在处理器执行的软件中进行算法实现。也就是说,即使设备的能量消耗具有数据依赖性,掩码技术也可以通过随机化密码设备所处理的中间值来消除该依赖关系。

在众多的掩码方案中,由于固定值掩码只占用少量的系统资源,因此适合于功耗低、面积小的单片机或智能卡等加密设备[13]。本文所采用的就是这种掩码方案,带掩码的 AES 算法基本工作流程如图 1所示。

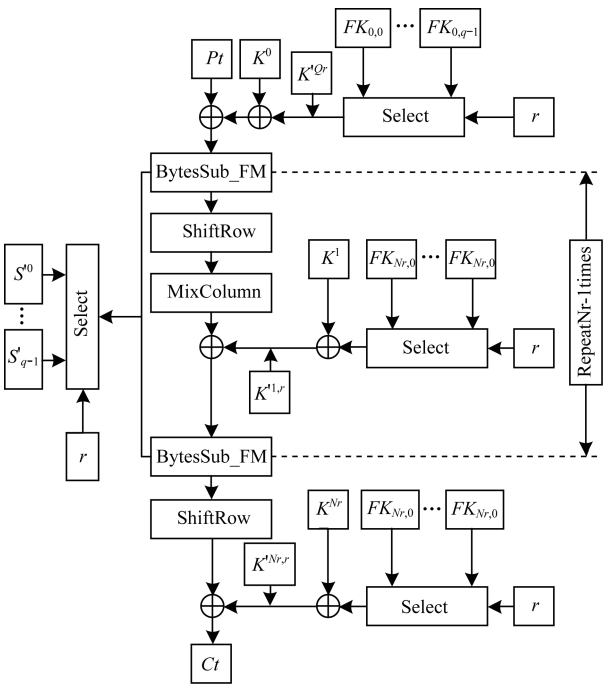

图 1　带掩码 AES 算法基本工作流程

带掩码 AES 算法伪代码如算法 1 所示。

算法 1　带掩码 AES 算法

```
Masked AES algorithm (Pt)
//K'i,r;masked subkey (i=0,1,…,Nr,r=0,1,…,q-1)
r = GenerateRandomNumber();
T' = Pt;
for (i=0;i<Nr-1;i++)
{
        T' = T' ⊕ K'i,r;
        T' = ByteSub_FM (T',r);
        T' = ShiftRow (T');
        T' = MixColumn (T');
}
T' = T'⊕K'Nr-1,r;
T' = ByteSub_FM (T',r);
T' = ShiftRow (T');
T' = T'⊕K'Nr,r;
Output T;
```

1.2　高阶 DPA 技术

高阶 DPA 攻击利用了某种联合泄漏,该联合泄漏基于出现在密码设备中的多个中间值。但是出于性能方面的考虑,掩码技术的典型实现是将同一个掩码应用于多个中间值,因此,在一个高效的算法实现中总会发生如下情况:一个掩码(或掩码的组合)及相应的掩码型中间值均会出现在设备中。因此,不需要研究一般意义上的高阶 DPA 攻击,仅仅利用与 2 个中间值相关的联合泄漏的高阶 DPA 攻击即可,这类攻击也称为二阶 DPA 攻击。这 2 个中间值既可以是同一个掩码所对应的 2 个掩码型中间值,也可以是掩码型中间值及相应的掩码。

一般而言,二阶 DPA 攻击不直接利用这种泄漏,因为这 2 个中间值通常出现在算法的不同操作中,所以它们可能被依次计算,并在不同时刻对能量消耗产生影响。在这种情况下,有必要对功耗曲线进行预处理,以便获得依赖于这 2 个中间值的能量消耗值。但是,即使这 2 个中间值同时会对能量消耗产生影响,对于所有假设而言,能量消耗的分布也可能具有相同的均值,而仅仅是方差有所不同。在这种情况下,使用传统统计方法的 DPA 攻击便不会成功,因为这些攻击方法都是基于均值的。为了成功地实施 DPA 攻击,就需要使用其他利用方差的统计方法,或者通过对功耗曲线进行预处理使得基于均值的方法能够生效。除此之外,二阶 DPA 攻击的工作方式与一阶 DPA 攻击完全相同。

1.3 预处理

在预处理环节,使用预处理函数 $pre(\ )$ 对每一条功耗曲线作预处理,可以得到一条预处理后的功耗曲线,一般称之为 $\tilde{t}$。

在实际攻击中,对攻击者真正有意义的是功耗曲线上分别对应于计算 u_m 和 v_m 的 2 个时间点。在通常情况下,并不知道计算这 2 个掩码中间值的准确时间,所以最多仅能猜测功耗曲线上一个大致的时间间隔 $I=t_{\tau+1},t_{\tau+2},\cdots,t_{\tau+l}$,并认为该区间可能包含了对 u_m 和 v_m 的计算。因此,实际上需要用预处理函数对该时间间隔内所有可能的 2 点组合都进行一次处理。如果使用的预处理函数是对称的,并且只考虑数据对 $(t_x,t_y)(x\neq y)$,则预处理后的功耗曲线包含了长度递减的 $l-1$ 段,即预处理后的功耗曲线的长度为:

$$(l-1)+(l-2)+\cdots+2+1=l\times(l-1)/2 \tag{1}$$

因此,一条经过预处理后的功耗曲线 $\tilde{t}$ 通常会由式(2)给出。

$$pre(t_{\tau+1},t_{\tau+2}),pre(t_{\tau+1},t_{\tau+3}),\cdots,pre(t_{\tau+2},t_{\tau+3}),\cdots,pre(t_{\tau+l-1},t_{\tau+l}) \tag{2}$$

到目前为止,相关研究人员已经提出了很多种预处理函数。常见的主要有 2 种:

第 1 种预处理函数由文献[2]提出,该函数计算两点之积:

$$pre(t_x,t_y)=t_x\times t_y \tag{3}$$

第 2 种最早在文献[15]中提出,是一种使用两点之和平方的方法:

$$pre(t_x,t_y)=(t_x+t_y)^2 \tag{4}$$

此外,文献[2]还指出,傅里叶变换也可用于对功耗曲线进行预处理。

2 理论基础

2.1 掩码技术的理论安全性

DPA 攻击之所以能够成功在于密码设备的瞬时能量消耗依赖于设备所处理的中间值,掩码破坏的目标也就是这种关系。例如中间值 v 被掩码保护,则与之对应的掩码型中间值 $v_m=v\times m$ 与 v 就不存在依赖关系,如果 v_m 与 v 没有依赖关系,则 v_m 对应的能量消耗与 v 也没有依赖关系。这样,掩码就实现了对一阶 DPA 攻击的良好抗性。从这种典型的掩码方案可以看出,每一个掩码型中间值都会导致一种在统计意义下不依赖于原始中间值的分布,这样带有掩码的密码算法就可以实现对一阶 DPA 攻击的抵御。例如,无论 v 为何值,$v\oplus m$ 总服从同样的分布,即 $v\oplus m$ 的分布与 v 不存在依赖关系。

2.2 联合假设中间值

对于高阶 DPA 来说,均假设攻击者利用了 2 个掩码型中间值 u_m 和 v_m 的联合分布。这意味着为了获得联合假设中间值 w,攻击者需要计算假设中间值 u 和 v,并将两者进行组合。因为针对的是采用固定值掩码方案的加密算法,所以组合函数肯定是异或函数,即 $w=u+v$。此外,因为可以从侧信道获得被攻击设备的汉明重量,所以可采用汉明重量模型将联合假设中间值 ω 映射为假设能量消耗值:

$$h=HW(w)=HW(u\oplus v) \tag{5}$$

在 DPA 攻击中,其第 5 步会对 $HW(u\oplus v)$ 和预处理后的功耗曲线进行比较,这意味着需要对 $\rho(H,\tilde{T})=\rho(HW(U\oplus V),\tilde{T})$ 进行估计。正确的密钥假设 k_{ck} 会导致在点 $\tilde{t}_{ct}$ 出现最大的相关系数。因此,$\rho_{ck,ct}$ 决定了攻击所需要的功耗曲线数量,又因为已经确定了所要采用的组合函数,所以相关性 $\rho_{ck,ct}$ 实际是由预处理函数决定的。点 $\tilde{t}_{ct}$ 对应于对 2 个目标中间值的处理,即 $\tilde{t}_{ct}=pre(HW(u_m),HW(v_m))$。因此,攻击的目标就可以简化为找到能够使式(6)取得最大值的预处理函数:

$$\rho(HW(u\oplus v),pre(HW(u_m),HW(v_m))) \tag{6}$$

2.3 预处理函数的选取

文献[7]表明,不同的预处理函数可能导致迥然不同的相关系数。根据文献[15]中的结论,可得不同预处理函数对相关系数 ρ 的影响,如表 1 所示。

表 1 不同预处理函数得到的相关系数

预处理函数	中间值位数为 1 bit	中间值位数为 2 bit	中间值位数为 3 bit	中间值位数为 4 bit
$pre(t_x,t_y)=t_x\times t_y$	-0.58	0.32	-0.17	-0.09
$pre(t_x,t_y)=(t_x+t_y)^2$	-0.33	-0.16	0.08	-0.04

由表 1 可知,在单比特的情况下,计算两点之积和计算两点之和平方的 2 种预处理函数均能取得非零值的相关系数,因此,基于这 2 个函数进行的预处理都是有效的。在多比特的情况下,计算两点之积的预处理函数效果要稍好于另一种方法,它在 4 bit 情况下获得的相关系数绝对值为 0.09,比计算两点之和平方的预处理方法高出 125%。

虽然 2 种方法都有一定效果,但其所获得的相关系数仍然偏小,导致攻击者必须使用更多的功耗曲线才能取得较好的攻击效果。为解决这一问题,文献[6]提出一种新的预处理函数规则,该函数计算两点之差的绝对值,即:

$$pre(t_x, t_y) = |t_x - t_y| \tag{7}$$

因为频繁地使用了这个预处理函数,所以称之为绝对差值函数。绝对差值函数更好地利用了各点之间的统计关系,较其他已知方法能更大程度地提高攻击的相关系数,具体效果如表 2 所示。

表 2　绝对差值预处理函数得到的相关系数

预处理函数	中间值位数为 1 bit	中间值位数为 2 bit	中间值位数为 3 bit	中间值位数为 4 bit
$pre(t_x, t_y) = \|t_x - t_y\|$	1.00	0.53	0.34	0.24

由表 2 可知,无论是单比特还是多比特的攻击场景,绝对差值预处理函数都能取得更为良好的攻击效果,在 4 bit 的情况下,相关系数仍能达到 0.24,远高于上述 2 种方法。

综上所述,不同的预处理函数会导致 DPA 攻击中不同的相关系数,至于哪一种预处理函数能取得最佳效果,则取决于所使用的能量模型。如果设备泄漏汉明重量,那么绝对差值函数是一个已知的最佳选择。因此,本文选择绝对差值作为预处理函数。

3　攻击方案设计

该攻击针对采用固定值掩码技术的 AES 算法。在该类型的掩码方案中,令 $m' = m$,这意味着 SubBytses 操作的输入和输出使用的是同一个掩码 m,而且该实现对 DPA 攻击来说是安全的。

3.1　功耗曲线的采集

把 AES 算法下载到自主开发的功耗数据采集平台中,该平台主要由一个 8 位的 mega16 单片机、电源电路和侧信道电压采集电路组成。收集 AES 运行期间的侧信道泄漏信息。示波器的 2 个探头一个与平台的触发信号管脚相连,另一个与数据信号管脚相连。数据采集平台和硬件总体配置分别如图 2、图 3 所示。

图 2　侧信道数据采集平台

图 3　硬件总体配置

3.2　功耗曲线预处理

任选一条 AES 运行时的功耗曲线,截取其第 1 轮 ~ 第 6 轮的数据并观察,如图 4 所示,根据曲线特点可以大致判断出 SubBytes 操作可能发生的时间区间在 340 ~ 400 之间,这一区间称之为“兴趣区间”。

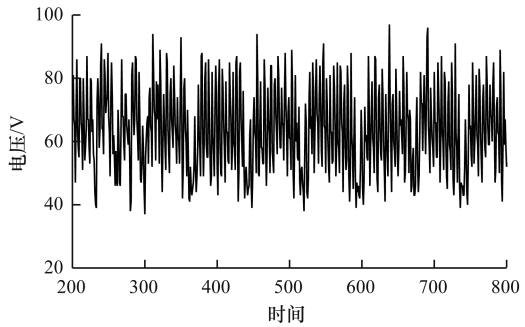

图 4　未经预处理的 AES 功耗曲线

对兴趣区间使用绝对差值的方法进行预处理,得到处理后的曲线如图 5 所示。

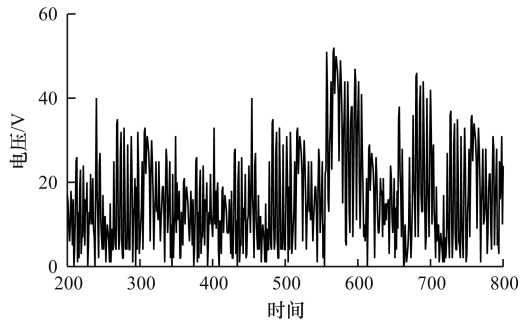

图 5　预处理之后的 AES 功耗曲线

3.3　攻击步骤

二阶 DPA 攻击仅仅是将 DPA 攻击应用于预处理后的功耗曲线,其具体攻击步骤如下:

步骤 1　选取攻击的中间值,本文选择字节替换异或操作的输入和输出值作为攻击点,该选择的优点在于可以在不知道掩码具体数值的情况下计算出所需要的中间值。

步骤 2　采集功耗曲线,并结合算法所使用的掩码技术进行相应的预处理。

步骤 3　计算中间值,对 256 个猜测的密钥分别计算其 S-box 输入前和输出后 2 次异或运算的结果。

步骤 4　计算芯片功耗的猜测值,使用汉明重量模型映射芯片运行时的功耗值。

步骤 5　计算相关系数,使用 DPA 计算每个猜测密钥对应的相关系数。

4　实验结果与分析

芯片中 AES 算法的实际密钥为 $key = 185$,分别对 480 原始功耗曲线和经过预处理的功耗曲线进行 DPA 攻击。

4.1　一阶 DPA 攻击结果

首先对采集到的功耗曲线应用一阶 DPA 攻击,256 种可能密钥值的全部攻击结果如图 6 所示,一阶 DPA 攻击所猜测出的正确密钥为 $key = 9$,如图 7 所示。

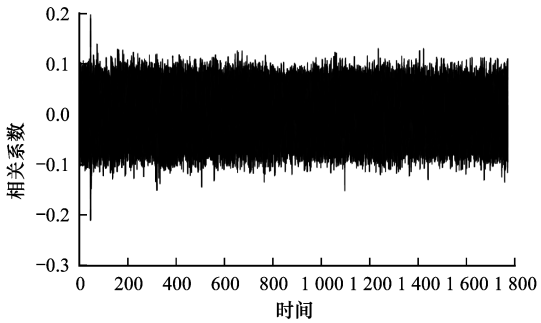

图 6 全部 256 种可能密钥的 DPA 攻击结果

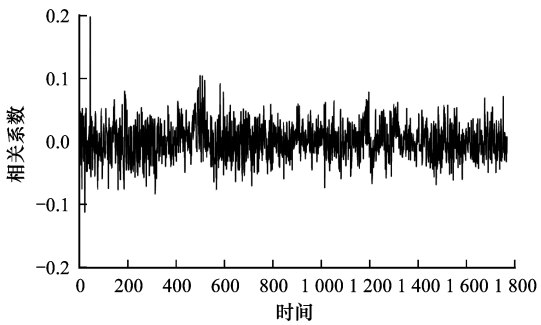

图 7 密钥 *key* = 9 时的攻击猜测

4.2 高阶 DPA 攻击结果

通过对功耗曲线进行直观分析,可以识别出 AES 算法第一轮所处位置。在第一轮中,取功耗曲线的第 340 个 ~ 第 400 个点作为兴趣区间,区间内共有 61 个点,这些点都处于可能包含了第 1 个 S-box 查表操作的时间间隔内。然后将预处理函数应用于该兴趣区间,根据第 1 节的结论,采用绝对差值作为预处理函数。因为该兴趣区间包含 61 个点,而预处理需要考虑 61 个点中所有两点的组合,所以预处理将产生一条包含 60 段的预处理后的功耗曲线,总计有 $61 \times (61-1)/2 = 1\,830$ 个点。

计算假设中间值 $u_{i,j} = d_i \oplus k_j$ 和 $v_{i,j} = S'(d_i \oplus k_j)$,并用异或函数将两者进行组合,得到 $w_{i,j} = u_{i,j} \oplus v_{i,j} = d_i \oplus k_j \oplus S'(d_i \oplus k_j)$。然后使用汉明重量模型按式(5)将其映射为假设能量消耗值 $h_{i,j}$:

$$h_{i,j} = HW(w_{i,j}) = HW((d_i \oplus k_j) \oplus S'(d_i \oplus k_j)) \tag{8}$$

最后对假设能量消耗和预处理功耗曲线进行比较。图 8 和图 9 给出了攻击结果。从图中可以看出,代表高相关性的尖峰出现在与处理 2 个被攻击中间值相关的所有位置,且该功耗曲线中的最高相关系数大约为 0.24,与表 1 中的理论结果 0.24 非常接近,进一步证明了攻击的有效性。因此,只需要使用大约 500 条功耗曲线就可将正确密钥与错误密钥明显区分开来。

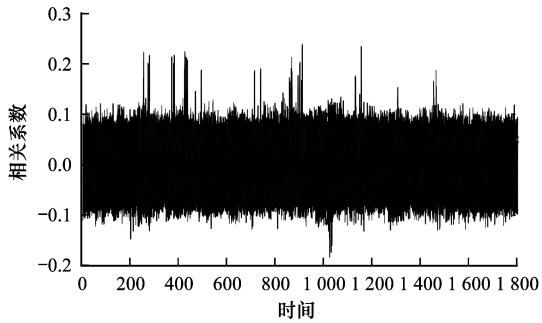

图 8 全部 256 种可能密钥的 HODPA 攻击结果

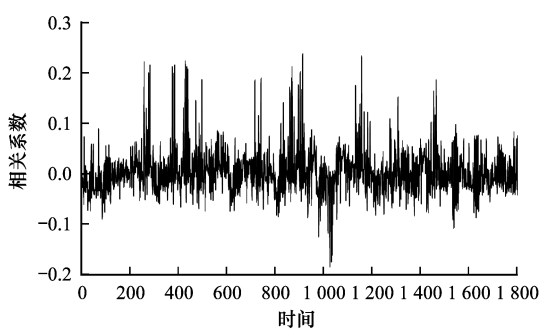

图 9 密钥 *key* = 185 时的攻击猜测

4.3 2 种攻击方法的对比及分析

2 种攻击方法的效果对比如表 3 所示。

表 3 攻击效果对比

攻击方法	正确密钥	正确密钥相关系数	猜测密钥	猜测密钥相关系数	使用功耗曲线数
一阶 DPA	185	0.147 3	9	0.201 4	480
高阶 DPA	185	0.242 1	185	0.242 1	480

从表 3 中可以看出,一阶 DPA 无法准确猜测出带掩码 AES 算法的正确密钥,另外,即使都使用了正确密钥进行攻击,其相关系数也仅能达到高阶 DPA 攻击效果的 60% 左右,且攻击结果之间严重缺乏区分度,没有实际的应用价值。

5 结束语

本文以带有固定掩码的 AES 加密算法为研究目标,结合掩码技术的具体特点,提出一种 HODPA 方案。选取科学的预处理函数,准确地判断兴趣区间的所在位置,并对其进行基于绝对差值的预处理。实验结果表明,本文攻击方案不仅降低计算的复杂度,而且可以提高攻击结果的相关系统。与传统 DPA 方案相比,实现了对带有掩码加密算法的成功攻击,且仅需要不到 500 条能量曲线就能取得较好的攻击效果,证明了该方案是有效的,并有较强的实用性。

参考文献

[1] 谭锐能,卢元元,田椒陵. 抗侧信道攻击的 SM4 多路径乘法掩码方法[J]. 计算机工程,2014,40(5):103-108.

[2] CHAIR S,JUTLA C S,RAO J R,et al. Towards Sound Approaches to Counteract Power-analysis Attacks[C]//Proceedings of IEEE CRYPTO'99. Washington D. C., USA:IEEE Press,1999:398-412.

[3] JOVAN D. TYMEN C. Multiplicative Masking and Power Analysis of AES [C]//Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer-Verlag, 2002:31-47.

[4] 徐　佩,傅　鹏. 防止差分功耗分析攻击的软件掩码方案[J]. 计算机应用研究,2016(1):245-248.

[5] MESSERGES T S. Using Second-order Power Analysis to Attack DPA Resistant Software[C]//Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer-Verlag, 2000:238-251.

[6] AKKAR M L,GOUBIN L. A Generic Protection Against High-order Differential Power Analysis[C]//Proceedings of International Workshop on Fast Software Encryption. Washington D. C.,USA:IEEE Press,2003:192-205.

[7] JOYE M, PAILLIER P, SCHOENMAKERS B. On Second-order Differential Power Analysis [C]// Proceedings of International Workshop on Cryptographic Hardware & Embedded Systems. Washington D. C., USA:IEEE Press,2005:293-308.

[8] Herbst C, Oswald E, Mangard S. An AES Smart Card Implementation Resistant to Power Analysis Attacks[C]// Proceedings of International Conference on Applied Cryptography and Network Security. Berlin, Germany: Springer-Verlag,2006:194-206.

[9] OSEALD E,MANGARD S,HERBST C,et al. Practical Second-order DPA Attacks for Masked Smart Card Implementations of Block Ciphers [M]. Berlin, Germany:Springer-Verlag,1970.

[10] YOO H S, HERBST C, MANGARD S, et al. Investigations of Power Analysis Attacks and Countermeasures for ARIA [J]. Lecture Notes in Computer Science,2007,4298:160-172.

[11] DING A A,ZHANG L,FEI Y,et al. A Statistical Model for Higher Order DPA on Masked Devices [C]// Proceedings of CHES'14. Berlin, Germany: Springer-Verlag,2014:147-169.

[12] DURVAUX F,STANDAERT F X. Efficient Selection of Time Samples for Higher-order DPA with Projection Pursuits[M]. Berlin,Germany:Springer-Verlag,2015.

[13] IYOH K, TAKENAKA M, TORII N. DPA Countermeasure Based on the "Masking Method" [C]// Proceedings of International Conference Seoul on Information Security & Cryptology. Washington D. C., USA:IEEE Press,2001:440-456.

[14] WADDLE J, WAGNER D. Towards Efficient Second-order Power Analysis[J]. Lecture Notes in Computer Science,2004,3156:1-15.

[15] 赵东艳,何　军. 针对密码算法的高阶 DPA 攻击方法研究[J]. 电子技术应用,2013,39(10):56-58.

编辑　索书志

(上接第 119 页)

[21] GEBOTYS C H, HO S, TIU C C. EM Analysis of Rijndael and ECC on a Wireless Java-based PDA[C]// Proceedings of CHES'05. Washington D. C., USA: IEEE Press,2005:250-264.

[22] FAN J, GIERLICHS B, VERCANTEREN F. To Infinity and Beyond: Combined Attack on ECC Using Points of Low Order[C]//Proceedings of CHES'11. Washington D. C.,USA:IEEE Press,2011:143-159.

[23] CHARI S,JUTLA C S,RAO J R,et al. Towards Sound Approaches to Counteract Power-analysis Attacks[C]// Proceedings of Advances in Cryptology-CRYPTO'99. Berlin,Germany:Springer,1999:398-412.

[24] CLAVIER C,JPYE M. Universal Exponentiation Algorithm: A First Step Towards Provable SPA-resistance [C]// Proceedings of CHES'01. Washington D. C., USA: IEEE Press,2001:300-308.

[25] TRICHINA E, BELLEZZA A. Implementation of Elliptic Curve Cryptography with Built-in Countermeasures Against Side Channel Attacks [C]//Proceedings of CHES'02. Washington D. C.,USA:IEEE Press,2002:98-113.

[26] 张金中,寇应展,陈财森,等. 二进制方法点乘的椭圆曲线密码故障攻击[J]. 计算机工程,2011,37(20):100-102.

[27] 马　博,包斯刚,戴显英. 智能卡中 ECC 抗功耗攻击方案的效率改进[J]. 计算机工程,2010,36(16):113-115.

[28] JOYE M,QUISQUATER J J. Protections Against Differential Analysis for Elliptic Curve Cryptography[C]//Proceedings of CHES'01. Washington D. C., USA: IEEE Press, 2001: 377-390.

[29] 王正义,赵俊阁. ECC 抗功率分析攻击的等功耗编码算法[J]. 计算机工程,2012,38(10):111-113.

[30] LEE J W, CHUNG S C, CHANG H C. An Efficient Countermeasure Against Correlation Power-analysis Attacks with Randomized Montgomery Operations for DF-ECC Processor [C]//Proceedings of CHES'12. Washington D. C., USA:IEEE Press,2012:548-564.

[31] 卢　宇,汪学明. 超椭圆曲线上斜——Frobenius 映射及有效标量乘算法研究[J]. 计算机工程,2017,43(6):78-83,91.

[32] HANKERSON D,MENEZES A,VANSTONE S. Guide to Elliptic Curve Cryptography[M]. Germany, Berlin: Springer,2004.

[33] SILVERMAN J H. The Arithmetic of Elliptic Curves[M]. Germany,Berlin:Springer,2009.

[34] 邬可可,李慧云,于峰崎. 对同步流密码设备的相关性功耗分析攻击[J]. 高技术通讯,2009,19(11):1142-1147.

编辑　索书志