分组密码抗 ASCA 安全性研究

李延斌[2] 唐 明[1),2)] 郭志鹏[2] 王龙龙[2] 胡晓波[3] 张焕国[1),2)]

[1)](武汉大学空天信息安全与可信计算教育部重点实验室 武汉 430072)

[2)](武汉大学计算机学院 武汉 430072)

[3)](北京南瑞智芯微电子科技有限公司 北京 102200)

摘 要 代数侧信道攻击(ASCA)已经成为一种对分组密码非常有效的分析方法.得到 ASCA 分析所需要的最少轮次,将有利于构造密码算法抗侧信道分析的轻量化防护策略.文中基于信息论方法,提出了一种在汉明重模型下评估分组密码抗 ASCA 安全性的方法,并给出了一种抗基于汉明重模型 ASCA 分析的安全性指标,称为汉明重扩散度(*HWE*),以度量分组密码的非线性部件及轮函数对抗 ASCA 分析的能力.文中从理论上证明了在同时考虑 ASCA 和线性分析或差分分析时,*HWE* 与非线性度以及差分均匀性这两项重要的密码学指标之间存在矛盾.因为差分均匀性和代数免疫度之间的关系,同理可知 *HWE* 和代数免疫度指标之间也存在矛盾.文中的实验结果表明,ASCA 方法分析 MIBS 算法时至少需要 4 个加密轮次,才有足够的泄漏信息满足 ASCA 中所有方程求解,与文中提出的理论度量结果一致.作者的研究工作从理论上对迭代型分组密码抗 ASCA 能力进行度量指标的设计与研究,研究结果发现现有分组密码具有 ASCA 的防御脆弱性.

关键词 代数侧信道分析;汉明重模型;非线性度;差分均匀性;代数免疫度;分组密码

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2016.00468

Study on the ASCA Resistance of Block Ciphers

LI Yan-Bin[2] TANG Ming[1),2)] GUO Zhi-Peng[2] WANG Long-Long[2]

HU Xiao-Bo[3] ZHANG Huan-Guo[1),2)]

[1)](*Key Laboratory of AIS&TC*, *Ministry of Education*, *Wuhan University*, *Wuhan* 430072)

[2)](*School of Computers*, *Wuhan University*, *Wuhan* 430072)

[3)](*NARI Group Corporation*, *Beijing* 102200)

Abstract The ASCA (Algebraic Side-Channel Attack) has become a very effective analytical method for block ciphers. Considering lightweight countermeasure, it would be helpful to know the minimal number of rounds needed in ASCA. In this paper, based on information theory, we present a method to evaluate the security of block ciphers against ASCA under the Hamming Weight model. We propose a security index referred to as *HWE* (Hamming Weight Extension) to measure the resistance of nonlinear operations and round functions of block ciphers to ASCA. Furthermore, we find that the *HWE* and two other important cryptographic indices, nonlinearity and differential uniformity, conflict with each other when ASCA and linear analysis or differential analysis are taken into account simultaneously. Considering the propositional relationship between differential uniformity and algebraic immunity, we find that the confliction between *HWE* and nonlinearity as well as differential uniformity and algebraic immunity. We present our experimental results with the MIBS algorithm and find that it needs to iterate at least 4 rounds of

收稿日期:2014-11-20;最终修改稿收到日期:2015-07-27.本课题得到国家自然科学基金(61472292,61202386)、金融 IC 卡及读写机具密码检测与安全防护技术研究及能力建设(2014ZX01032401-001)资助.**李延斌**,男,1992 年生,博士,主要研究方向为密码学、侧信道分析.E-mail:lyb9205@163.com.**唐 明**(通信作者),女,1976 年生,博士,副教授,主要研究方向为信息安全、密码学、密码芯片.E-mail:m.tang@126.com.**郭志鹏**,男,1992 年生,硕士,主要研究方向为密码学、侧信道分析.**王龙龙**,男,1988 年生,硕士,主要研究方向为密码学、侧信道分析.**胡晓波**,女,1977 年生,学士,主要研究方向为应用密码学、安全芯片.**张焕国**,男,1945 年生,教授,主要研究领域为信息安全、密码学、可信计算、容错计算.

the MIBS to guarantee that the HWE of both nonlinear operations and round functions are nonzero, which are consistent with our analysis.

Keywords　algebraic side-channel attack; Hamming weight model; nonlinearity; differential uniformity; algebraic immunity; block cipher

1　引　言

代数侧信道攻击(简称 ASCA)是由 Standaert 等人[1-2]在 2009 年提出的一种对分组密码通用的分析方法. 它的原理是将代数攻击和侧信道攻击[3-5]结合到一起,从而使攻击者可以对未知密钥建立出一些可以用来恢复密钥的方程.

Renauld 等人[1,6]研究了 PRESENT[1]和 AES[6]对抗 ASCA 的安全性问题,并用 zChaff SAT 求解器[7]恢复了所有未知密钥. Renauld 等人[8]研究了影响 ASCA 成功率的因素. 文献[9]中,Oren 等人提出了一种有更高容错率的新的代数密码分析方法. Zhao 等人[7]提出了一种新的 ASCA 方法,提高了其在实际应用中的有效性. Carlet 等人[10]研究了 ASCA 分别在汉明重和汉明距模型下的有效性问题.

获得 ASCA 所需要的最少轮次对于改善密码算法设计非常有利. 由于汉明重模型[1,8-9,11]是 ASCA 中最通用的泄漏模型之一,并且可以很容易的扩展到汉明距离模型,因此本文基于汉明重模型提出了一种评估分组密码抵抗 ASCA 的安全性的方法. 基于对 ASCA 的安全性分析,我们还提出了一种度量 ASCA 的安全性指标,称为汉明重扩散度(HWE),以度量分组密码非线性部件和轮函数对 ASCA 的抵抗能力. 我们研究了 HWE 和非线性度、差分均匀性这两个重要的密码学指标之间的关系,并证明了分组密码非线性部件和轮函数不能同时抵抗 ASCA 和非线性分析或差分分析的攻击.

Guilley 等人[12]从两个布尔信号(Boolean signals)相关性系数的角度研究了单比特 DPA:第 1 个布尔信号依赖于 S 盒输出比特,第 2 个布尔信号依赖于功耗. 他们指出 S 盒抵抗线性分析的安全性越高就越容易遭受侧信道攻击,如 DPA[5]. 我们在本文中扩展了 Guilley 等人的研究:在汉明重功耗模型下[13]研究多比特 DPA. 文献[12-13]说明了经典密码学指标和 DPA 特性不能同时满足. 我们通过 HWE 与非线性度或差分均匀性的相互矛盾证明了 ASCA 和经典密码学分析的矛盾,并说明了 ASCA 的对抗策略可以破坏 SCA 方程的建立.

本文第 2 节我们介绍一种评估 ASCA 所需要加密轮次数的方法;基于这种方法我们给出 HWE 的定义,并在第 3 节讨论 HWE 与非线性度和差分均匀性的关系;第 4 节介绍关于 MIBS 算法的 ASCA 实验,同时说明 HWE 和评估的有效性;最后是全文的总结.

2　评　估

2.1　主要思想

ASCA 是结合了代数分析和侧信道攻击,通过建立两类方程最终恢复出密钥的分析方法. 我们分别命名这两类方程为 A 类方程和 B 类方程. A 类方程描述了目标加密算法的代数方程;B 类方程刻画了目标算法在泄漏模型下的信息泄漏. 对于目标算法第 1 轮的方程建立说明见图 1.

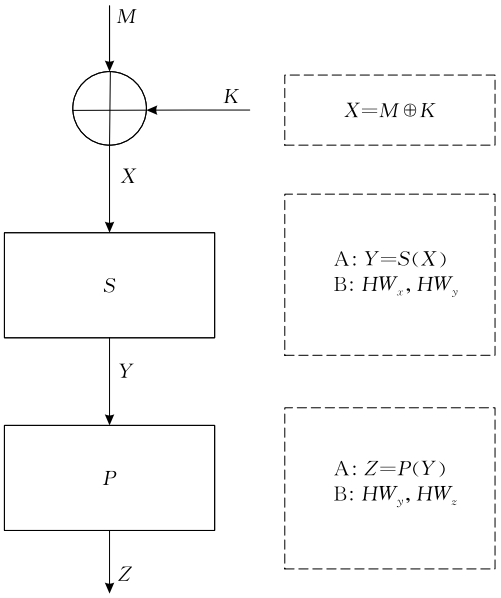


图 1　单轮次 A、B 类方程示意图

由 $X=M\oplus K$ 可知(其中,K 表示密钥,为 ASCA 的攻击目标),对于已知的明文攻击,密钥提取的分析过程可以等价为对 X 的恢复. 对于给定 x,我们记 HW_x 为 x 的汉明重. 根据汉明重量信息的采集阶段不同,X 的信息量的提取包括下面 3 个部分:

第 1 部分:已知 HW_x,直接恢复 X 的信息量.

我们选择汉明重最后两个比特来保证代数函数阶数小于 3,以限制文献[14]中代数函数的多项式数量;

第 2 部分:由 HW_x,HW_y 及 $Y=S(X)$,能恢复的 X 的信息量;

第 3 部分:由 HW_y,HW_z 及 $Z=P(Y)$,能恢复的 Y 的信息量,再将此 Y 与第 2 部分得到的 X,利用 $Y=S(X)$进行筛选,能恢复 X 的信息量.

本文用一轮加密运算的所有中间状态对应的 B 类方程和 A 类方程,所能恢复 X 的信息量来定量表示一轮加密运算的信息泄露量.

2.2 一轮的信息泄漏量

考虑以下几种情况下的信息泄漏.

首先,当明文 M 是已知的,X 的信息量等价于密钥 K 的信息量.假设明文 M 是服从正态分布的,并且当明文 M 已知时,X 和 K 有相同的概率分布.

对于一个给定的随机变量 X,H_X 表示 X 的熵:

$$H_X=-\sum p\{X=x\}\log_2 p\{X=x\}.$$

其次,X 的信息泄漏是由它的汉明重引起的.

定义 1. 若已知 X 的汉明重量 HW_x,则恢复 X 的信息量可由以下条件熵计算得到

$$H_0=H_{X|M}-H_{X|HW_x}=H_{X|M}-\sum_{hw_x\in HW_x}p(hw_x)H(X|HW_x=hw_x),$$

其中:

HW_x 表示采样到的 X 中间状态的汉明重量集合,hw_x 为该集合中的元素;

$p(hw_x)$ 表示某个具体汉明重量取值对应出现的概率.

第三,泄漏估计量由一些中间结果的汉明重取值决定.

定义 2. 对于加密部件 $Y=OP(X)$,已知 X 和 Y 的汉明重量,则推导出 X 的信息量可用下述条件熵表示:

$$H_{X|M}-H_{X|A}=H_{X|M}-\sum_{a\in A}p(a)H_{X|A=a},$$

其中:

A 表示汉明重量二元组(HW_x,HW_y)的集合;

a 表示 A 中的元素,对应一组特定的 X,Y 的汉明重量取值.

定义 3. 已知 X,Y,Z 的汉明重量及 $Y=OP_1(X)$,$Z=OP_2(Y)$,则由汉明重量能确定 X 的信息量,可表示为

$$H_{X|M}-H_{X|B}=H_{X|M}-\sum_{b\in B}p(b)H_{X|B=b},$$

其中:

OP_1,OP_2 分别表示轮函数中的非线性部件和线性部件;

B 表示 X,Y,Z 的汉明重量组合(HW_x,HW_y,HW_z)集合,b 为 B 中的元素.

更多比特的汉明重和线性部件的扩散特性将会大大增加计算复杂度,$H_{X|M}-H_{X|B}$将会由于计算复杂度太大而无法在计算机上运行.

2.3 ASCA 所需分析轮次的估算方法

本节要解决的问题是:"ASCA 需要多少轮次加密来收集足够的泄漏才能恢复所有的密钥比特?"

(1)各轮子密钥随机独立

由于加密算法中密钥扩展算法的随机性,可将每轮的子密钥视为独立,分别设为 $k_1,k_2,k_3,\cdots,k_n,k_1$ 为初始密钥.由于密钥扩展算法是由 k_1 生成对应的各轮子密钥,所以最终分析目标仍为初始密钥 k_1.

(2)两轮加密中的信息泄露

设 m 为一轮输出的比特数,n 为经过一轮 ASCA 后密钥中仍未知的比特数.则两轮 ASCA 后失败的概率为

$$\left(1-\frac{P_{m-n}^n}{P_m^n}\right),$$

P_m^n 表示从 m 个元素中选择 n 个元素的序列数,$n\leq m$.

(3)一些轮次中的信息泄漏

我们展示了一种计算 ASCA 所需轮次数的方法.计算轮次数的步骤如下:

① $P_{k,j}$ 表示 ASCA 经过 k 轮次后有 j 比特未知的概率,则有

$$\sum_{j=0}^{n}P_{k,j}=1,$$

因此,经过 k 轮后未知比特的概率为 P_k,有 $P_k=1-P_{k,0}$.

② 对于第 1 轮,当 $0\leq j\leq n$,$P_{1,j}=0$,并且 $P_{1,n}=0$.显然,$P_1=1$.

③ 对于任意轮次 k,有

$$P_{k,j}=\sum_{i=j}^{n}P_{k-1,i}\times\frac{C_i^jC_{m-i}^{n-j}}{C_m^n},\ 0\leq j\leq n,$$

C_m^n 表示从 m 个元素中选择 n 个元素的所有组合数.

根据上述方法,我们就可以计算出 $P_{k,j}$.

3 抗 ASCA 的分组密码非线性部件

3.1 汉明重扩散度

定义 4. 对任意的运算部件 OP,我们定义其汉明重扩散度为

$$HWE=H_{(HW_X,HW_Y)}-H_0,$$

其中，H_0 同定义 1，表示已知运算部件输入汉明重量时的信息量.

定理 1.　汉明重扩散度具有非负性，当且仅当某一个 $p_{ij}=p_i$，其余 p_{ij} 均为 0 时，HWE 为 0. 其中，p_{ij} 表示运算部件 OP 输入值的汉明重为 i，输出值的汉明重为 j 的概率；p_i 表示运算部件 OP 输入值的汉明重为 i 的概率.

证明.　设 OP 为从 F_{2^n} 到 F_{2^n} 的映射. 对于任何 $X\in F_{2^n}$，都有 $Y=OP(X)\in F_{2^n}$. 为了保证代数函数阶数少于 3，我们选择汉明重值的最后两比特.

如果 X 的汉明重 HW_x 可以被看作是一个随机变量，则 HW_x 的概率分布由 HW_x 的比特数 n 决定，具体定义如表 1 所示，计算其熵为 $H_0=-\sum_{i=0}^{n}p_i\log_2 p_i$. 在本文下面的内容中，我们选择汉明重的两比特来建立 B 类方程.

表 1　*OP* 输入数据的汉明重概率分布

HW_x	P_r
00	p_0
01	p_1
10	p_2
11	p_3

如果一个汉明重量对 (HW_x,HW_y) 可以被看成是一个随机变量，则 (HW_x,HW_y) 的概率分布由运算部件 OP 决定. 其分布如表 2 所示.

表 2　*OP* 输入与输出的汉明重概率分布

HW_y	HW_x				p_i
	00	01	10	11	
00	p_{00}	p_{01}	p_{02}	p_{03}	p_0
01	p_{10}	p_{11}	p_{12}	p_{13}	p_1
10	p_{20}	p_{21}	p_{22}	p_{23}	p_2
11	p_{30}	p_{31}	p_{32}	p_{33}	p_3

其中，$p_i=p_{i0}+p_{i1}+p_{i2}+p_{i3}$.

记 $f(x)$ 表示映射 $f(x)=-x\log_2 x$.

当 $0\le x_1,x_2,x_1+x_2\le 1$ 时，$f(x_1)+f(x_2)\ge f(x_1+x_2)$. 并且当且仅当 $x_1=0$ 或者 $x_2=0$ 时，等号成立.

由于 $p_{i0}+p_{i1}+p_{i2}+p_{i3}=p_i$，所以

$$f(p_{i0})+f(p_{i1})+f(p_{i2})+f(p_{i3})\ge f(p_i),$$

并且当且仅当某一个 p_{ij} 和 p_i 相等，其他 p_{ij} 均为 0 时，等号成立.

记 $H_{(HW_x,HW_y)}$ 表示 (HW_x,HW_y) 的熵. 则

$$H_{(HW_x,HW_y)}=\sum_{i=0}^{n}f(p_{i0})+f(p_{i1})+f(p_{i2})+f(p_{i3})\ge\sum_{i=0}^{n}f(p_i)=H_0.$$

根据以上分析，可以得到：当且仅当只有其一个 p_{ij} 等于 p_i，其他 p_{ij} 均为 0 时，

$$\sum_{i=0}^{n}f(p_{i0})+f(p_{i1})+f(p_{i2})+f(p_{i3})=\sum_{i=0}^{n}f(p_i).$$

证毕.

3.2　*HWE* 和非线性度间关系

为了评估对抗汉明重模型下的 ASCA 的抵抗性，我们引入了安全性指标 HWE. 分组密码算法中的非线性部件是算法的核心，关系到整个算法的安全性，对于非线性部件设计安全性的常见密码学指标主要包括：非线性度、差分均匀性、代数免疫度等. 其中非线性度是衡量非线性部件抗线性分析能力的重要指标，我们首先研究 HWE 和非线性度间的关系. 它们都与加密过程的中间值的汉明重有关.

(1) 分析非线性部件 HWE 和非线性度在特定规模 S 盒(Sbox)中存在的矛盾.

考虑 4×4 Sbox 的 HWE 与非线性度的关系. 4×4 Sbox 输入 X 的汉明重 HW_x 分布见表 3.

表 3　4×4 Sbox 输入数据的汉明重概率分布

HW_x	P_r
00	2/16
01	4/16
10	6/16
11	4/16

在 HWE 为 0 的条件下，(HW_x,HW_y) 的分布只有如下两种情况，见表 4 和表 5.

表 4　4×4 Sbox 输入与输出的汉明重概率分布 1

HW_y	HW_x			
	00	01	10	11
00	2/16	0	0	0
01	0	4/16	0	0
10	0	0	6/16	0
11	0	0	0	4/16

表 5　4×4 Sbox 输入与输出的汉明重概率分布 2

HW_y	HW_x			
	00	01	10	11
00	2/16	0	0	0
01	0	0	0	4/16
10	0	0	6/16	0
11	0	4/16	0	0

对于两种情况都满足 $HW_x(\mathrm{mod}2)=HW_y(\mathrm{mod}2)$，也就是说 4×4 Sbox 输入和输出的汉明重的奇偶性保持不变.

定理 2.　4×4 Sbox 的 HWE 为 0 必然导致

Sbox 非线性度也为 0.

证明. 设

$$X=(x_1,x_2,x_3,x_4)\in F_{2^4},$$

$$Y=(y_1,y_2,y_3,y_4)\in F_{2^4}.$$

令 $u_0=(1,1,1,1)$,点乘 $u_0\cdot OP(X)$ 表示两者逐比特相乘然后再相加,该式得到的是从 F_{2^4} 到 F_2 的映射.

设 L_4 是从 F_{2^4} 到 F_2 的所有仿射函数构成的集合,取 L_4 中的一个元素:

$$l_0(X)=(x_1,x_2,x_3,x_4),$$

那么,

$$\begin{aligned}&d_H(u_0\cdot OP(X),l_0(X))\\&=d_H(y_1+y_2+y_3+y_4,x_1+x_2+x_3+x_4)\\&=d_H(hw_y(\mathrm{mod}2),hw_x(\mathrm{mod}2))=0,\end{aligned}$$

所以,

$$\begin{aligned}N_F&=\min_{l(X)\in L_4,u\in L_4,u\neq 0}d_H(u_0\cdot OP(X),l(X))\\&\leq d_H(u_0\cdot OP(X),l_0(X))=0,\end{aligned}$$

又因为 $N_F\geq 0$,因此 $N_F=0$. 证毕.

考虑 8×8 Sbox 的 HWE 与非线性度的关系. 8×8 Sbox 输入 X 的汉明重 HW_x 分布见表 6.

表 6 8×8 Sbox 输入数据的汉明重概率分布

HW_x	P_r
00	9/32
01	8/32
10	7/32
11	8/32

在 HWE 为 0 的条件下,(HW_x,HW_y) 的分布只有如下两种情况,见表 7 和表 8.

表 7 8×8 Sbox 输入与输出的汉明重概率分布 1

HW_y	HW_x			
	00	01	10	11
00	9/32	0	0	0
01	0	8/32	0	0
10	0	0	7/32	0
11	0	0	0	8/32

表 8 8×8 Sbox 输入与输出的汉明重概率分布 2

HW_y	HW_x			
	00	01	10	11
00	9/32	0	0	0
01	0	0	0	8/32
10	0	0	7/32	0
11	0	8/32	0	0

这两种情况也都满足 $HW_x(\mathrm{mod}2)=HW_y(\mathrm{mod}2)$. 如上所述,同样可以证明其非线性度为 0,即 8×8 Sbox 的 HWE 为 0 时,其非线性度也为 0.

(2) 分析 HWE 和非线性度在规模无限制的非线性部件中存在矛盾.

由于迭代型分组密码的轮函数可以看成无规模限制的非线性部件,非线性部件的安全策略同样适用于轮函数.

记 n 为一个正整数,表示 S 盒的规模大小. 我们将 OP 的规模 n 按模 4 分成以下 4 类,并用定理 3 至定理 6,对每种规模下的 HW_x 的概率分布(即 p_0,p_1,p_2,p_3)进行论证.

定理 3. 当 $n=4k$(k 是正整数)时,$p_0\neq p_1$,$p_0\neq p_3$,$p_2\neq p_1$,$p_2\neq p_3$.

证明. 令

$$\begin{aligned}B_0^n&=C_n^0+C_n^4+\cdots+C_n^{n-4}+C_n^n,\\B_1^n&=C_n^1+C_n^5+\cdots+C_n^{n-3},\\B_2^n&=C_n^2+C_n^6+\cdots+C_n^{n-2},\\B_3^n&=C_n^3+C_n^7+\cdots+C_n^{n-1}.\end{aligned}$$

那么,$p_0=\frac{B_0^n}{2^n}$,$p_1=\frac{B_1^n}{2^n}$,$p_2=\frac{B_2^n}{2^n}$,$p_3=\frac{B_3^n}{2^n}$.

因此,只要证明各个 B_i^n 之间的关系即可.

显然有 $B_1^n=B_3^n$,而且 $B_1^n+B_3^n=B_0^n+B_2^n$,因此,

$$B_0^n\neq B_2^n,\ B_0^n\neq B_1^n,\ B_2^n\neq B_1^n \tag{1}$$

如果上述 3 个不等式中的任意一个成立那么另外两个也成立. 下面利用数学归纳法证明式(1)对任意的 $n=4k$ 也是成立的.

当 $n=4$ 时,容易验证式(1)成立. 假定对于 $n-4$ 的情况式(1)成立. 那么当 n 任意时,

$$\begin{aligned}B_2^n=&(\underline{C_{n-1}^1}+C_{n-1}^2)+\underline{(C_{n-1}^5}+C_{n-1}^6)+\cdots+\\&\underline{(C_{n-1}^{n-3}}+C_{n-1}^{n-2}),\\B_1^n=&(C_{n-1}^0+\underline{C_{n-1}^1})+(C_{n-1}^4+\underline{C_{n-1}^5})+\cdots+\\&(C_{n-1}^{n-4}+\underline{C_{n-1}^{n-3}})\end{aligned} \tag{2}$$

下划线的项相互抵消掉,剩下的部分分别记为 R_2^1,R_1^1,那么只需要考虑 R_2^1,R_1^1 是否相等.

$$\begin{aligned}R_2^1=&(C_{n-2}^1+\underline{C_{n-2}^2})+(C_{n-2}^5+\underline{C_{n-2}^6})+\cdots+\\&(C_{n-2}^{n-3}+\underline{C_{n-2}^{n-2}}),\\R_1^1=&\underline{C_{n-1}^0}+(C_{n-2}^3+\underline{C_{n-2}^4})+\cdots+(C_{n-2}^{n-5}+\underline{C_{n-2}^{n-4}})\end{aligned} \tag{3}$$

下划线的项相互抵消(是倒序相消的),剩下的部分分别记为 R_2^2,R_1^2,现在只需要考虑 R_2^2,R_1^2 是否相等.

$$\begin{aligned}R_2^2=&(C_{n-3}^0+C_{n-3}^1)+(C_{n-3}^4+C_{n-3}^5)+\cdots+\\&(C_{n-3}^{n-4}+C_{n-3}^{n-3})\\=&C_{n-4}^0+(C_{n-4}^0+\underline{C_{n-4}^1})+\underline{(C_{n-4}^3}+C_{n-4}^4)+\\&(C_{n-4}^4+\underline{C_{n-4}^5})+\cdots+(\underline{C_{n-4}^{n-5}}+C_{n-4}^{n-4})+C_{n-4}^{n-4},\\R_1^2=&(C_{n-3}^2+C_{n-3}^3)+(C_{n-3}^6+C_{n-3}^7)+\cdots+\\&(C_{n-3}^{n-6}+C_{n-3}^{n-5})\\=&\underline{(C_{n-4}^1}+C_{n-4}^2)+(C_{n-4}^2+\underline{C_{n-4}^3})+\end{aligned}$$

$$(\underline{C_{n-4}^5}+C_{n-4}^6)+(C_{n-4}^6+\underline{C_{n-4}^7})+\cdots+$$
$$(\underline{C_{n-4}^{n-7}}+C_{n-4}^{n-6})+(C_{n-4}^{n-6}-\underline{C_{n-4}^{n-5}}).$$

下划线的项相互抵消，剩下的部分分别记为 R_2^3，R_1^3，现在只需要考虑 R_2^3，R_1^3 是否相等.

$$R_2^3=2(C_{n-4}^0+C_{n-4}^4+\cdots+C_{n-4}^{n-4})=2B_0^{n-4},$$
$$R_1^3=2(C_{n-4}^2+C_{n-4}^6+\cdots+C_{n-4}^{n-6})=2B_2^{n-4}.$$

由假设知道 $B_0^{n-4}\neq B_2^{n-4}$，因此 $B_1^n\neq B_2^n$，因此式(1)对任意的 $n=4k$ 都成立. 证毕.

定理 4. 当 $n=4k-1$(k 是正整数)时，$p_0=p_3$，$p_1=p_2$，$p_0\neq p_1$.

证明. 令

$$B_0^n=C_n^0+C_n^4+\cdots+C_n^{n-3},$$
$$B_1^n=C_n^1+C_n^5+\cdots+C_n^{n-2},$$
$$B_2^n=C_n^2+C_n^6+\cdots+C_n^{n-1},$$
$$B_3^n=C_n^3+C_n^7+\cdots+C_n^n.$$

显然 $B_0^n=B_3^n$，$B_1^n=B_2^n$. 容易看出式(3)中的 R_2^1，R_1^1 对应于这里的 B_2^n，B_0^n，由定理 3 的证明过程知道 $R_2^1\neq R_1^1$，因此 $B_2^n\neq B_0^n$，$B_0^n\neq B_1^n$. 证毕.

定理 5. 当 $n=4k-2$(k 是正整数)时，$p_0\neq p_1$，$p_0\neq p_3$，$p_2\neq p_1$，$p_2\neq p_3$.

证明. 令

$$B_0^n=C_n^0+C_n^4+\cdots+C_n^{n-6}+C_n^{n-2},$$
$$B_1^n=C_n^1+C_n^5+\cdots+C_n^{n-5}+C_n^{n-1},$$
$$B_2^n=C_n^2+C_n^6+\cdots+C_n^{n-4}+C_n^n,$$
$$B_3^n=C_n^3+C_n^7+\cdots+C_n^{n-3}.$$

显然 $B_0^n=B_2^n$. 而且有 $B_1^n+B_3^n=B_0^n+B_2^n$. 因此如果 $B_0^n\neq B_3^n$，$B_0^n\neq B_1^n$，$B_1^n\neq B_3^n$ 中的任意一个不等式成立，那么另外两个也成立. 把 B_3^n，B_1^n 同时加上 $C_n^0+C_n^4+C_n^8+\cdots+C_n^{n-2}$，则

$$B_3^n+C_n^0+C_n^4+C_n^8+\cdots+C_n^{n-2}$$
$$=C_n^0+(C_n^3+C_n^4)+(C_n^7+C_n^8)+\cdots+(C_n^{n-3}+C_n^{n-2})$$
$$=C_{n+1}^0+C_{n+1}^4+C_{n+1}^8+\cdots+C_{n+1}^{n-2}=B_0^{n+1},$$
$$B_1^n+C_n^0+C_n^4+C_n^8+\cdots+C_n^{n-2}$$
$$=(C_n^0+C_n^1)+(C_n^4+C_n^5)+\cdots+(C_n^{n-2}+C_n^{n-1})$$
$$=C_{n+1}^1+C_{n+1}^5+\cdots+C_{n+1}^{n-1}=B_1^{n+1}.$$

由定理 3 的证明可以知道 $B_0^{n+1}\neq B_1^{n+1}$，因此 $B_3^n\neq B_1^n$. 证毕.

定理 6. 当 $n=4k-3$(k 是正整数)时，$p_0=p_1$，$p_2=p_3$，$p_0\neq p_2$.

证明. 令

$$B_0^n=C_n^0+C_n^4+\cdots+C_n^{n-5}+C_n^{n-1},$$
$$B_1^n=C_n^1+C_n^5+\cdots+C_n^{n-4}+C_n^n,$$
$$B_2^n=C_n^2+C_n^6+\cdots+C_n^{n-3},$$
$$B_3^n=C_n^3+C_n^7+\cdots+C_n^{n-2}.$$

显然有 $B_0^n=B_1^n$，$B_2^n=B_3^n$. 把 B_0^n，B_2^n 两边同时加上 B_1^n，则

$$B_0^n+B_1^n=(C_n^0+C_n^1)+(C_n^4+C_n^5)+\cdots+(C_n^{n-1}+C_n^n)$$
$$=C_{n+1}^1+C_{n+1}^5+\cdots+C_{n+1}^n=B_1^{n+1},$$
$$B_2^n+B_1^n=(C_n^1+C_n^2)+(C_n^5+C_n^6)+\cdots+$$
$$(C_n^{n-4}+C_n^{n-3})+C_n^n$$
$$=C_{n+1}^2+C_{n+1}^6+\cdots+C_{n+1}^{n+1}=B_2^{n+1}.$$

由定理 4 的证明过程可以知道 $B_1^{n+1}\neq B_2^{n+1}$，因此 $B_0^n\neq B_2^n$. 证毕.

由定理 3 至定理 6 可知，当 n 给定，$p_0\neq p_1$，$p_0\neq p_3$，$p_2\neq p_1$，$p_2\neq p_3$. 为了证明这个结论和非线性度的关系，我们有以下结论.

定理 7. 对于运算部件 OP，如果对任意的 $X\in F_{2^n}$，有 $HW_X\equiv HW_{OP(X)}(\mathrm{mod}\,2)$，那么 OP 的非线性度为 0.

证明. 设

$$X=(x_1,x_2,\cdots,x_n)\in F_{2^n},$$
$$Y=(y_1,y_2,\cdots,y_n)\in F_{2^n}.$$

$u_0=(1,1,\cdots,1)$，点乘 $u_0\cdot OP(X)$ 表示两者逐比特相乘然后再相加，该式得到的是从 F_{2^n} 到 F_2 的映射.

设 L_n 是从 F_{2^n} 到 F_2 的所有仿射函数构成的集合，取 L_n 中的一个元素：$l_0(X)=x_1+x_2+\cdots+x_n\in L_n$，那么，

$$d_H(u_0\cdot OP(X),l_0(X))$$
$$=d_H(y_1+y_2+\cdots+y_n,x_1+x_2+\cdots+x_n)$$
$$=d_H(HW_y(\mathrm{mod}\,2),HW_x(\mathrm{mod}\,2))=0.$$

所以，

$$N_{OP}=\min_{l(X)\in L_n,u\in L_n,u\neq 0}d_H(u_0\cdot OP(X),l(X))$$
$$\leq d_H(u_0\cdot OP(X),l_0(X))=0.$$

又因为 $N_{OP}\geq 0$，因此 $N_{OP}=0$. 证毕.

定理 8. 对于运算部件 OP，如果对任意的 $X\in F_{2^n}$，有 $HW_X\neq HW_{OP(X)}(\mathrm{mod}\,2)$，那么 OP 的非线性度为 0.

证明. 与定理 7 的证明类似，取

$$l_0(X)=x_1+x_2+\cdots+x_n.$$

对于运算部件 OP，如果存在 F_{2^n} 的非空真子集 A，使得对任意的 $X\in A$，有

$$HW_X\equiv HW_{OP(X)}(\mathrm{mod}\,2).$$

当对任意的 $X\in B=F_{2^n}-A$，有

$$HW_X\neq HW_{OP(X)}(\mathrm{mod}\,2),$$

那么 OP 的非线性度大于或者等于 0. 证毕.

由定理 2,7,8 可知,当 HWE 为 0 且 OP 的规模给定时,OP 的非线性度也为 0. 这意味着非线性部件和确定规模的轮函数都不能同时抵抗 ASCA 和线性分析. 另外,由于非线性度越小,代数免疫度越小[15],所以 HWE 和代数免疫度同样存在矛盾.

3.3 *HWE* 和差分均匀性间的关系

定理 9 提出了 HWE 和差分均匀性间的矛盾关系.

定义 5. 称 $2^n\times 2^m$ 阶矩阵 $\boldsymbol{\omega}(S)$ 为 $n\times m$ 代换盒 $S(x)$ 的差分分布矩阵;

如果 $\boldsymbol{\omega}=\begin{pmatrix}\lambda_{0,0} & \cdots & \lambda_{0,2^m-1}\\ \cdots & \cdots & \cdots\\ \lambda_{2^n-1,0} & \cdots & \lambda_{2^n-1,2^m-1}\end{pmatrix}$,其中 $\lambda_{ij}=|\{x\in GF(2)^n|S(x)\oplus S(x\oplus\alpha_i)=\beta_j\}|$,$i=0,1,\cdots,2^n-1$,$j=0,1,\cdots,2^m-1$. 这里 α_i,β_j 分别为 i,j 的二进制表示.

定义 6. 设 $n\times m$ 代换盒 S 的差分分布矩阵为 $\boldsymbol{\omega}(S)=(\lambda_{ij})$,则称

$$\begin{aligned}\delta(S)&=\max\{\lambda_{i,j}|i=0,1,\cdots,2^n-1,j=0,1,\cdots,2^m-1\}\\&=\max\{|\{x\in GF(2)^n|S(x)\oplus S(x\oplus\alpha)=\beta,\\&\quad\alpha\in GF(2)^n,\alpha\neq 0,\beta\in GF(2)^m\}|\}\end{aligned}$$

为 S 的差分均匀度. 为了抗击差分攻击,代换盒的差分均匀度 $\delta(S)$ 应当越小越好.

定理 9. 对于任意 $n\times m$ Sbox,HWE 为 0 必然导致 Sbox 差分均匀度最大.

证明. 设 x 为 Sbox 的输入,$S(x)$ 为 Sbox 的输出. α 和 β 同定义 6. 由于 HWE 为 0,根据定理 2 可知,

$$HW_x(\mathrm{mod}2)=HW_{S(x)}(\mathrm{mod}2).$$

根据 α 和 β 的汉明重的奇偶性进行分类讨论:

(1) $HW_\alpha(\mathrm{mod}2)=HW_\beta(\mathrm{mod}2)=0(\mathrm{mod}2)$

根据 HW_x 奇偶性再对所有的 x 进行分类:

若 $HW_x(\mathrm{mod}2)=0(\mathrm{mod}2)$,

有 $HW_{x\oplus\alpha}(\mathrm{mod}2)=0(\mathrm{mod}2)$.

则 $HW_{S(x)}(\mathrm{mod}2)=0(\mathrm{mod}2)$,

$HW_{S(x\oplus\alpha)}(\mathrm{mod}2)=0(\mathrm{mod}2)$.

可以得到

$$HW_{S(x)\oplus S(x\oplus\alpha)}(\mathrm{mod}2)=0(\mathrm{mod}2)=HW_\beta(\mathrm{mod}2).$$

所以,对于所有符合 $HW_x(\mathrm{mod}2)=0(\mathrm{mod}2)$ 的 x 均满足定义 6 中的等式.

若 $HW_x(\mathrm{mod}2)=1(\mathrm{mod}2)$,

有 $HW_{x\oplus\alpha}(\mathrm{mod}2)=1(\mathrm{mod}2)$.

则 $HW_{S(x)}(\mathrm{mod}2)=1(\mathrm{mod}2)$,

$HW_{S(x\oplus\alpha)}(\mathrm{mod}2)=1(\mathrm{mod}2)$.

可以得到

$$HW_{S(x)\oplus S(x\oplus\alpha)}(\mathrm{mod}2)=0(\mathrm{mod}2)=HW_\beta(\mathrm{mod}2),$$

所以,对于所有符合 $HW_x(\mathrm{mod}2)=1(\mathrm{mod}2)$ 的 x 均满足定义 6 中的等式.

同理可得

(2) $HW_\alpha(\mathrm{mod}2)=HW_\beta(\mathrm{mod}2)=1(\mathrm{mod}2)$

对于所有符合 $HW_x(\mathrm{mod}2)=0(\mathrm{mod}2)$ 的 x 均满足定义 6 中的等式.

对于所有符合 $HW_x(\mathrm{mod}2)=1(\mathrm{mod}2)$ 的 x 均满足定义 6 中的等式.

(3) $HW_\alpha(\mathrm{mod}2)=1(\mathrm{mod}2)$,$HW_\beta(\mathrm{mod}2)=0(\mathrm{mod}2)$

对于所有符合 $HW_x(\mathrm{mod}2)=0(\mathrm{mod}2)$ 的 x 均不满足定义 6 中的等式.

对于所有符合 $HW_x(\mathrm{mod}2)=1(\mathrm{mod}2)$ 的 x 均不满足定义 6 中的等式.

(4) $HW_\alpha(\mathrm{mod}2)=0(\mathrm{mod}2)$,$HW_\beta(\mathrm{mod}2)=1(\mathrm{mod}2)$

对于所有符合 $HW_x(\mathrm{mod}2)=0(\mathrm{mod}2)$ 的 x 均不满足定义 6 中的等式.

对于所有符合 $HW_x(\mathrm{mod}2)=1(\mathrm{mod}2)$ 的 x 均不满足定义 6 中的等式.

综上所述,在(1)和(2)的情况下,符合定义 6 中等式的 x 的个数为

$$Max=\{x|x\in GF(2)^n\}.$$

对应得到 $\delta(S)=Max$. 对于其他的一般情形,都有 $\delta(S)\leq Max$. 证毕.

根据定理 9,我们可以得出如下结论:当 HWE 为 0 时,差分均匀性最大. 这意味着非线性部件和轮函数不能同时抵抗 ASCA 和差分攻击.

当 4×4 Sbox 的 HWE 为 0,一共可以构造出 2!×4!×6!×4!种 Sbox,其中符号!表示阶乘. 对于其中每一种 Sbox 进行差分均匀性计算,我们得到最小的差分均匀性为 14,比一般情况下的 Sbox 差分均匀性要大. 这说明了对于 4×4 Sbox,HWE 为 0 导致了 Sbox 对抗差分攻击的能力减弱.

4 实 验

4.1 ASCA 轮次度量实验

4.1.1 随机抽取样本方法的合理性验证实验

实验目的:证明用随机抽取样本的方法来计算熵值的正确性,在复杂度允许的情况下,得到的结果与理论值接近.

实验方法:已知 HW_z,HW_y,且 $Z=Y_1\oplus Y_2\oplus Y_3\oplus Y_4\oplus Y_5$,每次实验根据汉明重量分布的概率随

机抽取 10000 个样本来模拟汉明重量分布，独立重复实验 20 次.

实验结果：运行随机取样的程序统计 20 次，结果见表 9，熵值为 10 时共 10 次，熵值为 11 时共 10 次，由计算可知样本熵值的期望为 10.5.

表 9　熵的均值

实验次数	熵均值
1	11
2	10
3	10
4	10
5	11
6	11
7	10
8	11
9	10
10	11
11	11
12	11
13	10
14	11
15	11
16	11
17	10
18	10
19	10
20	10

结果分析：精确熵值为 10.4334，这与通过随机取样计算得到的估计值基本一致. 因此，我们可以用随机取样的方法去估计 ASCA 中一轮的泄漏信息量.

4.1.2　随机抽取估计一轮的泄漏信息量

实验目标：利用 4.1.1 节中随机取样的方法对 MIBS 算法[16]进行实验，估计其一轮的泄漏信息量.

实验方法：已知 HW_x，HW_y，HW_z 以及 $Y=\mathrm{Sbox}(X)$，$Z=P(Y)$，选择 20000 个以上的随机明文作为样本，独立进行 10 次实验，统计一轮 MIBS 算法中泄露 X 的信息量.

实验结果：见表 10.

结果分析：根据一轮 MIBS 的信息泄露量，当置信度≥99%时，ASCA 分析建立方程的轮次至少需要 4 轮. 这里需要说明的是实验所需的轮次远远小于 MIBS 算法的总轮次，这意味着 4 轮中的信息泄漏量已经足够用来恢复全部密钥. 该结果与 4.2 节实验中针对 MIBS 算法进行实际 ASCA 分析的结果一致.

表 10　熵的均值

实验次数	$H_{X\mid B}$	期望
1	1.46439	1.154206
2	1	
3	1	
4	1.02832	
5	1.02832	
6	1.5	
7	1.02832	
8	1.02832	
9	1	
10	1.46439	

MIBS 的结构如图 2 所示.

置换层为 S：$F_{2^4}\to F_{2^4}$：$x_i\to y_i=s(x_i)$，其中 $1\le i\le 8$.

混合层为 M：$(GF(2)^4)^8\to(GF(2)^4)^8$

$(y_8,y_7,\cdots,y_1)\to(y'_8,y'_7,\cdots,y'_1)$

$y'_1=y_2\oplus y_3\oplus y_4\oplus y_5\oplus y_6\oplus y_7$，

$y'_2=y_1\oplus y_3\oplus y_4\oplus y_6\oplus y_7\oplus y_8$，

$y'_3=y_1\oplus y_2\oplus y_4\oplus y_5\oplus y_7\oplus y_8$，

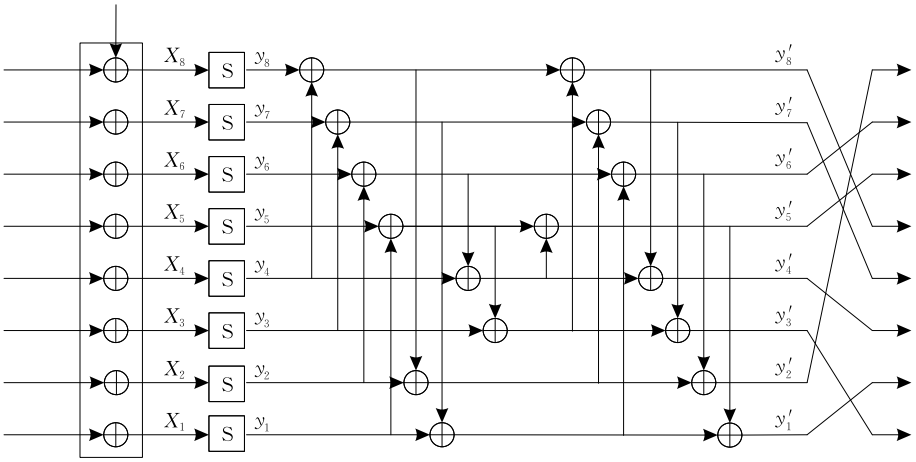


图 2　MIBS[16]的轮函数

$y_4' = y_1 \oplus y_2 \oplus y_3 \oplus y_5 \oplus y_6 \oplus y_8$,
$y_5' = y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_6$,
$y_6' = y_1 \oplus y_2 \oplus y_3 \oplus y_6 \oplus y_7$,
$y_7' = y_2 \oplus y_3 \oplus y_4 \oplus y_7 \oplus y_8$,
$y_8' = y_1 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_8$.

4.2 针对 MIBS 算法的 ASCA 分析

实验目的:利用 ASCA 对 MIBS 算法进行分析;验证 4.1.2 节对 ASCA 分析方法泄露信息量的定量分析结论.

实验方法:实验包括以下 3 个步骤:

第 1 步(offline phase 1):对加密算法的代数方程进行描述.

目的是把加密算法转化为大型的低阶方程系统,从而把密钥的恢复工作转变为方程的求解.我们将这一阶段建立的代数方程称为 A 类方程.

第 2 步(online phase):在线采集侧信道信息.

我们利用示波器在 SASEBO-GII 上利用 Zhao 等人[7]的方法提取 MIBS 加密过程中的中间值的汉明重.

我们选择汉明重模型来建立与侧信道泄漏有关的泄漏方程.我们将此阶段建立的基于汉明重模型的方程,称为 B 类方程.

第 3 步(offline phase 2):方程求解.

一旦方程系统和推论都得到了,剩下的工作就是求解方程.可以利用很多方法求解,包括 XL、Grobner 基、SAT 求解器等方法.

实验结果分析:本文以 MIBS 算法为例,利用基于汉明重量泄露模型的 ASCA 分析方法进行攻击,方程求解器为 SAT-Solver——CryptoMinisat2.9.0①,最终分析结果见表 11.

表 11 ASCA 对 MIBS 的攻击结果

实验类型	求解时间/s	解的唯一性
4 轮 ASCA	0.76	唯一解
4 轮代数攻击	无法在有效时间内求解	无
4 轮 ASCA,无密钥扩展	2.21	不唯一解
3 轮 ASCA	0.61	不唯一解

说明:如表 11 中结果所示,针对 MIBS 加密算法需要 4 轮 ASCA 方可得到唯一正确解,所需轮次与 2.3 节中理论上推到出的轮次数目一致.实验结果验证了本文提出针对汉明重泄露模型的 ASCA 定量分析评估方法的有效性.

5 结 论

本文研究了 ASCA 所需分组密码加密轮次的估算方法.研究的动机包括两个方面:第一,ASCA 分析所需轮次数可以看作是一种分组密码对抗 ASCA 的安全性评价指标;第二,知道 ASCA 所需轮次数对通过加轻量化对抗来改善密码算法设计有很大帮助.

我们在研究 ASCA 分析分组密码所需轮次的过程中定义了 HWE 指标,用于评估分组密码抵抗 ASCA 的安全性.当 HWE 为 0,它表示输入的信息泄露和输出的信息泄漏相等.这说明在本轮 ASCA 过程中没有增加其他新的信息泄漏.

有趣的是,我们发现并证明了当给定部件的规模时,HWE 和分组密码非线性度、差分均匀性以及代数免疫度间存在矛盾.这意味着满足密码学指标的现有分组密码算法不能同时抵抗 ASCA.这也就意味着现有分组密码算法理论上存在抗 ASCA 的脆弱性,这意味着对抗 ASCA 分析方法需要从算法设计实现角度上进一步开展研究.

参 考 文 献

[1] Renauld M, Standaert F X. Algebraic side-channel attacks// Proceedings of the Inscrypt 2009. Beijing, China, 2009: 393-410

[2] Standaert F X, Malkin T G, Yung M. A unified framework for the analysis of side channel key recovery attacks// Proceedings of the 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cologne, Germany, 2009: 443-461

[3] Boneh D, DeMillo R A, Lipton R J. On the importance of checking cryptographic protocols for faults//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Konstanz, Germany, 1997: 37-51

[4] Kocher P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems//Proceedings of the 16th Annual International Cryptology Conference Santa Barbara. California, USA, 1996: 104-113

[5] Kocher P, Jaffe J, Jun B. Differential power analysis// Proceedings of the 19th Annual International Cryptology Conference Santa Barbara. California, USA, 1999: 388-397

[6] Renauld M, Standaert F X, Veyrat-Charvillon N. Algebraic side-channel attacks on the AES: Why time also matters in DPA//Proceedings of the Cryptographic Hardware and Embedded Systems. Lausanne, Switzerland, 2009: 97-111

[7] Zhao X, Zhang F, Guo S, et al. MDASCA: An enhanced algebraic side-channel attack for error tolerance and new leakage model exploitation//Proceedings of the Constructive

① CryptoMiniSat 2.9.0 released. http://www.msoos.org/2011/01/cryptominisat-2-9-0-release, 2010,6,10

Side-Channel Analysis and Secure Design. Darmstadt, Germany, 2012: 231-248

[8] Renauld M, Standaert F X. Representation, leakage and cipher-dependencies in algebraic side-channel attacks// Proceedings of the ACNS 2010 Industrial Track. Beijing, China, 2010: 1-15

[9] Oren Y, Kirschbaum M, Popp T, et al. Algebraic side channel analysis in the presence of errors//Proceedings of the Cryptographic Hardware and Embedded Systems. California, USA, 2010: 428-442

[10] Carlet C, Faugere J C, Goyet C, et al. Analysis of the algebraic side channel attack. Journal of Cryptographic Engineering, 2012, 2(1): 45-62

[11] Bogdanov A, Kizhvatov I, Pyshkin A. Algebraic methods in side-channel collision attacks and practical collision detection //Proceedings of the 9th International Conference on Cryptology in India. Kharagpur, India, 2008: 251-265

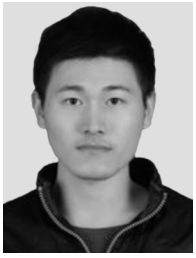
[12] Guilley S, Hoogvorst P, Pacalet R. Differential power analysis model and some results//Proceedings of the IFIP 18th World Computer Congress TC8/WG8.8 &TC11/WG11.2 Sixth International Conference on Smart Card Research and Advanced Applications (CARDIS). Toulouse, France, 2004: 22-27

[13] Prouff E. DPA Attacks and S-Boxes//Gilbert H, Handschuh H eds. Fast Software Encryption. LNCS 3557. Berlin Heidelberg: Springer, 2005: 424-441

[14] Courtois N T, Pieprzyk J. Cryptanalysis of block ciphers with overdefined systems of equations//Proceedings of the 8th International Conference on the Theory and Applications of Cryptology and Information Security. Queenstown, New Zealand, 2002: 267-287

[15] Meng Qiang, Chen Lu-Sheng, Fu Fang-Wei. The relation ship between algebraic immunity and nonlinearity//Proceedings of the 15th China Information Theory Society Annual Conference. Qingdao, China, 2008: 405(in Chinese)
(孟强，陈鲁生，符方伟. 代数免疫度与非线性度之间的关系//中国电子学会第十五届信息论学术年会暨第一届全国网络编码学术年会. 青岛，中国，2008：405)

[16] Izadi M, Sadeghiyan B, Sadeghian S S, et al. MIBS: A new lightweight block cipher//Garay J A, Miyaji A, Otsuka A eds. Cryptology and Network Security. LNCS 5888. Springer, Heidelberg, 2009: 334-348



LI Yan-Bin, born in 1992, Ph. D. candidate. His research interests include side channel analysis and cryptanalysis.

TANG Ming, born in 1976, Ph. D., associate professor. Her research interests include information security, cryptography and cryptographic chip.

GUO Zhi-Peng, born in 1992, M. S. His research interests include side channel analysis and cryptanalysis.

WANG Long-Long, born in 1988, M. S. His research interests include side channel analysis and cryptanalysis.

HU Xiao-Bo, born in 1977, bachelor. Her research interests include cryptographic design and cryptographic chip.

ZHANG Huan-Guo, born in 1945, professor. His research interests include information security, cryptography, trusted computing and fault-tolerant computing.

Background

The ASCA researched in this paper was proposed in 2009. It combines algebraic analysis and side-channel attacks to establish equations aiming to recover secret keys, and has become one of the most effective side-channel attacks. At present, the research about ASCA mainly focuses on two aspects: make the ASCA applied on more ciphers, improve the ASCA's universal property and how to establish side-channel equation withstand much higher measurement error rates, improve the effectiveness of ASCA. This paper aims at improving the countermeasures design of cipher, researches the resistance of ASCA in nonlinear operations of block ciphers and evaluates the minimal number of rounds needed in ASCA in theory according to cryptographic indices of nonlinear operations of block ciphers. On this basis, we propose a security index referred to as *HWE* (Hamming Weight Extension) to measure the resistance of nonlinear operations and round functions of block ciphers to ASCA. Our analysis shows that the confliction between *HWE* and nonlinearity as well as differential uniformity and algebraic immunity.

Our research team has successively used power, electromagnetic and fault analysis different structure of block ciphers in SCA for 8 years. And proposed using evolution ciphers improve block ciphers' resistance of ASCA. We completed a prototype system about side-channel analysis, protection and testing.

This research is supported by the National Natural Science Foundation of China (61472292, 61202386). It aims at putting forward a set of lightweight countermeasure scheme against side-channel analysis, to achieve the unification of light weight and security. This research is also supported by the Project of Research and Capacity Building on Cryptography Detection and Security Protection Technology on Financial IC Card and Read-Write Device (2014ZX01032401-001).