DOI:10.16157/j.issn.0258-7998.2013.10.022

针对密码算法的高阶 DPA 攻击方法研究

赵东艳,何 军
(北京南瑞智芯微电子科技有限公司,北京 100192)

摘 要:差分能量分析(DPA)是一种强大的密码算法攻击技术。一种有效的防御措施是对参与运算的中间数据进行掩码,然而采用掩码技术的密码算法仍然可以用高阶 DPA 进行攻击。高阶 DPA 攻击与一般 DPA 攻击相比较存在很多难点,包括建立正确的攻击模型、选取正确的攻击点、构造适当的组合函数以及提高攻击模型的信噪比等。通过对一种经典的掩码方案进行分析,逐一阐述在高阶 DPA 攻击中如何解决上述难点,并在硬件实现的算法协处理器上对攻击方法进行了验证。

关键词:高阶 DPA 攻击;差分能量分析;侧信道分析
中图分类号:TP309 **文献标识码**:A **文章编号**:0258-7998(2013)10-0056-03

Investigation of high order DPA against cryptographic algorithm

Zhao Dongyan, He Jun
(Beijing NARI SmartChip Microelectronics Company Limited, Beijing 100192, China)

Abstract: Differential power analysis is a powerful attack against cryptographic algorithms. An effective protection method is to mask the intermediate data during calculation. However, cryptographic algorithms with masking technology are still susceptible to high order DPA. Compared with normal DPA, there are more difficulties to be solved in high order DPA such as correct attack modeling, right choices of attack points, right construction of composition function and ways of improving s/n rate, etc. In this paper, by analyzing a classic masking scheme, we will demonstrate how to solve the difficulties mentioned above during a high order DPA attack, and then verify it on a hardware-implemented cryptographic coprocessor.

Key words: high order DPA; differential power analysis; side channel analysis

近几年来,针对密码算法的 DPA 攻击得到越来越多的关注。通过对设备的功耗进行分析发现,密码设备在执行相同指令的情况下,功耗与参与运算的密钥有一定的关系。攻击者利用这种关系对采集到的能量迹进行 DPA 攻击,可以分析出密钥[1-3]。

为了防御 DPA 攻击,一种有效的技术是对参与运算的数据进行随机掩码,也称为信息盲化[4]。加了掩码的数据在进行密码运算时,包含密钥信息的中间数据被掩码保护起来,因此能够抵抗一阶 DPA 攻击。然而这种防御技术仍然可以用高阶 DPA 进行攻击。相对一阶 DPA 攻击来说,高阶 DPA 需要攻击者了解更多的算法实现细节,并且需要选择恰当的攻击模型,所以攻击过程也比一阶 DPA 复杂得多。

1 能量泄露模型和 DPA 攻击原理

1.1 能量泄露模型

设备的功耗可以通过在设备的 GND 管脚和地之间插入一个电阻,然后用示波器测量电阻两端的电压变化来获得。为了建立能量泄露模型,用 $P[t]$ 表示设备在特定 t 时刻的功耗。$P[t]$ 可以分成两部分,第一部分是与运算相关的功耗 $d[t]$,第二部分是所有与运算无关的功耗 n,包括常量部分以及各种噪声。因此 $P[t]$ 可以表示为[5]:

$$P[t]=a\cdot d[t]+n \tag{1}$$

其中 a 是刻画 $d[t]$ 对 $P[t]$ 贡献度的常量系数。

在指令相同的情况下,与运算相关的功耗 $d[t]$ 可以用中间数据的汉明重量表示,即:

$$d[t]=W[D] \tag{2}$$

其中 D 是密码算法在 t 时刻的中间值。

根据式(1)、式(2),设备的能量泄露模型可以表示为:

$$P[t]=a\cdot W[D]+n \tag{3}$$

如果 D 是均匀分布的随机变量,长度为 m 位,则 $W[D]$ 的期望为 $\mu_W=m/2$、方差为 $\sigma_W^2=m/4$。在统计学理论上,引入功耗 P 和汉明重量之间的相关系数 ρ_{PW} 来表示上述

线性模型的匹配度：

$$\rho_{PW}=\frac{\mathrm{cov}(P,W)}{\sigma_P\sigma_W}=\frac{a\sigma_W}{\sigma_P}=\frac{a\sqrt{m}}{\sqrt{ma^2+4\sigma_n}} \tag{4}$$

如果在 m 位中仅 s 位是可预测的，则功耗和汉明重量之间的偏相关系数为：

$$\rho_{PW_s}=\frac{a\sqrt{s}}{\sqrt{ma^2+4\sigma_n}}=\rho_{PW}\sqrt{\frac{s}{m}} \tag{5}$$

上述相关系数在中间值汉明重量完全正确时达到最大值。

1.2 DPA 攻击原理

DPA 的攻击理论正是利用功耗与中间值之的相关性，对密码算法的一小段子密钥进行穷举，然后计算在该假设密钥下中间值汉明重量 W' 和功耗 P 之间的相关系数。当相关系数达到最大值时，可以推断出假设的子密钥为正确密钥。中间值汉明重量和功耗之间的相关系数计算如下：

$$\rho_{PW'}=\frac{N\Sigma P_iW'_i-\Sigma P_i\Sigma W'_i}{\sqrt{N\Sigma P_i^2-(\Sigma P_i)^2}\ \sqrt{N\Sigma W_i^2-(\Sigma W_i)^2}} \tag{6}$$

1.3 高阶 DPA 攻击

1.3.1 高阶 DPA 攻击原理

高阶 DPA 攻击的思想是在进行 DPA 攻击时，同时考虑一条能量迹曲线上的 k 个点。这 k 个点对应了 k 个不同的中间值，应用组合函数将 k 个中间值组合成一个中间值，然后对新生成的中间值进行 DPA 攻击，这种攻击称为 k 阶 DPA 攻击[6]。

1.3.2 高阶 DPA 攻击的组合函数

组合函数的选择已有相关文献进行过讨论[6]。常见的组合函数包括乘积函数、绝对差函数以及和平方函数等。对于二阶 DPA 攻击来说，乘积函数计算两点之积，即 $\mathrm{comp}(t_x,t_y)=t_x\cdot t_y$；绝对差函数计算两点之差的绝对值，即 $\mathrm{comp}(t_x,t_y)=|t_x-t_y|$；和平方函数计算两点之和的平方，$\mathrm{comp}(t_x,t_y)=(t_x+t_y)^2$。

在二阶 DPA 攻击中，假设被攻击的设备采用布尔掩码，组合假设中间值为 $\xi=\xi_1\oplus\xi_2$。如果设备泄露汉明重量，可以采用汉明重量模型将组合假设中间值映射为假设功耗值：

$$h=\mathrm{HW}(\xi)=\mathrm{HW}(\xi_1\oplus\xi_2) \tag{7}$$

分别用 $\mathrm{HW}(\xi_1)$ 和 $\mathrm{HW}(\xi_2)$ 代表能量迹上 t_x 和 t_y 两点的真实功耗，两点的真实功耗通过组合函数生成组合功耗 P：

$$P=\mathrm{comp}(t_x,t_y)=\mathrm{comp}(\mathrm{HW}(\xi_1),\mathrm{HW}(\xi_2)) \tag{8}$$

由此可以计算出假设功耗值和组合功耗之间的相关系数：

$$\rho_{h,P}=\rho(\mathrm{HW}(\xi_1\oplus\xi_2),\mathrm{comp}(\mathrm{HW}(\xi_1),\mathrm{HW}(\xi_2))) \tag{9}$$

比较相关系数在不同组合函数以及不同中间值位数情况下的差异，可以确定各种组合函数的优劣。

从表 1 可以看出，在泄露汉明重量的情况下，使用绝对差组合函数能达到更好的效果。

表 1 不同情况下的相关系数

组合函数	ξ 的位数			
	1	2	3	4
$\mathrm{comp}(t_x,t_y)=t_x\cdot t_y$	−0.58	0.32	−0.17	−0.09
$\mathrm{comp}(t_x,t_y)=\lvert t_x-t_y\rvert$	1.00	0.53	0.34	0.24
$\mathrm{comp}(t_x,t_y)=(t_x+t_y)^2$	−0.33	−0.16	0.08	−0.04

2 掩码技术和高阶 DPA 攻击

2.1 掩码技术原理

掩码技术的核心思想是使密码设备的功耗不依赖于设备所执行的密码算法的中间值。掩码技术通过随机化密码设备所处理的中间值来实现这个目标。掩码方案可以用下式来表示：

$$\xi_m=\xi * m \tag{10}$$

其中 ξ 表示密码运算过程中的中间值；m 是掩码，通常是一个内部产生的随机数；ξ_m 是经过掩码的掩码中间值；运算 $*$ 通常根据密码算法所使用的操作进行定义，一般为布尔“异或”运算、模加运算或者模乘运算。

2.2 DES 掩码方案

下面介绍一种经典的 DES 变形掩码方案[4]。在算法开始时，消息通过 64 bit 的随机数使用布尔“异或”运算进行掩码。该掩码方案的关键是在每轮开始都带上 X1 的掩码，为了实现这个目标，掩码方案对 S 盒进行了修改。修改后的 S 盒满足以下输入输出关系：

$$\mathrm{SMBOX}(A)=\mathrm{SBOX}(A\oplus X2)\oplus P^{-1}(X1_{0-31}\oplus X1_{32-63}) \tag{11}$$

其中 P^{-1} 表示 P 置换的逆过程。掩码方案在最后的 FP 置换之前，将结果“异或”X，消除掩码得到正确的加密结果。计算过程如图 1 所示。

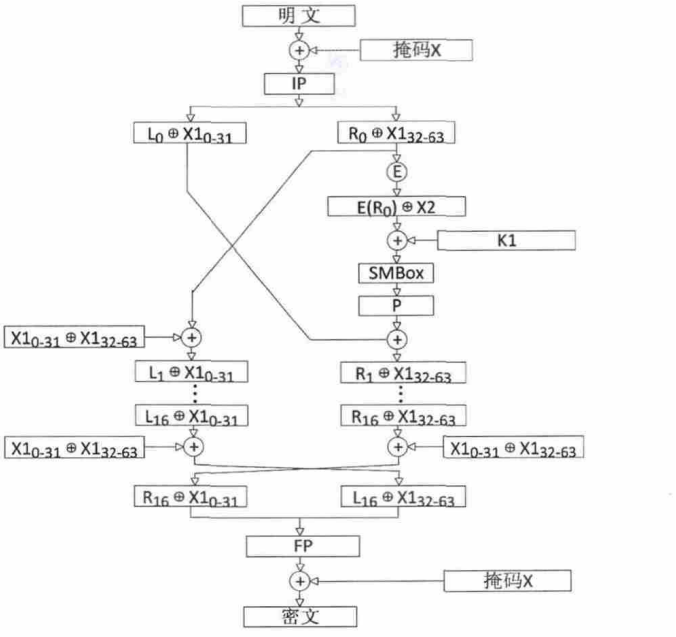

图 1 变形掩码方案运算过程

2.3 变形掩码方案的高阶 DPA 攻击

在上述掩码方案中，整个加密过程每个中间值都带着掩码，因此可以抵抗一阶 DPA 攻击。掩码方案为了保证每轮运算的结构相同，在轮运算结束时通过非线性的 SBOX 变换将掩码重新设置为每轮开始的的掩码值 $X1_{32-63}$。

根据高阶 DPA 攻击的原理，可以选择第一轮开始和结束的中间值作为攻击对象，将两点“异或”后得到不带掩码的中间值 $\xi=R_0\oplus R_1=L_0\oplus R_0\oplus P(SBox(E(R_0)\oplus K_1))$，如图 2 所示。

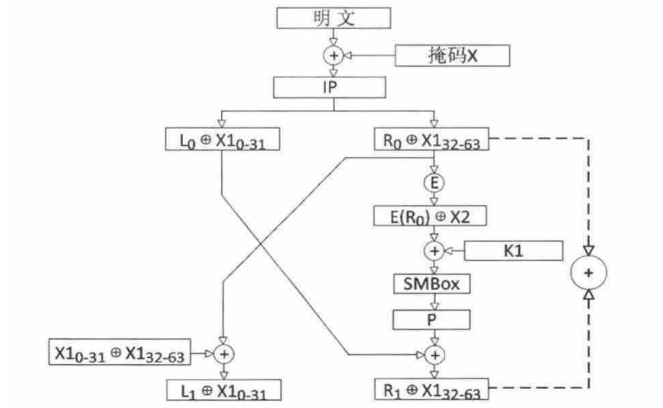

图 2 二阶 DPA 攻击的组合中间值

在 S 盒的运算结果经过 P 置换后，每个字节都和所有的 48 bit 子密钥有关，如图 3 所示。因此不能直接选择单个输出字节作为中间值。

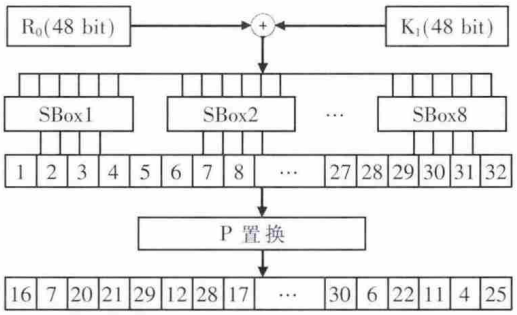

图 3 第一轮运算 P 置换后的输出结果

在硬件密码设备中，DES 协处理器中每轮运算的 8 个 S 盒实现是并行的，每个 S 盒的输出占 P 置换后的4 bit (1/8 长度)，因此不管 S 盒输出在 P 置换后位置如何变化，其对能量的影响是始终存在的。如果以一个 S 盒的 6 bit 子密钥作为攻击目标，那么在 P 置换输出结果中除了该 S 盒的 4 bit 输出外，其余 28 bit 输出结果都是噪声。

根据前述的能量泄露模型，6 bit 的密钥假设可以达到的最大相关系数为：

$$\rho_{PW_s}=\rho_{PW}\sqrt{\frac{s}{m}}=\rho_{PW}\sqrt{\frac{4}{32}}=0.35\rho_{PW} \quad (12)$$

即猜测 6 bit 密钥时相关系数是猜测全部密钥的 0.35 倍。为了提高信噪比，可以选择同时攻击 12 bit 密钥，即 2 个 S 盒的密钥。在这种情况下，相关系数可以提高到猜测全部密钥的 0.5 倍，信噪比会大大提高。

$$\rho_{PW_s}=\rho_{PW}\sqrt{\frac{s}{m}}=\rho_{PW}\sqrt{\frac{8}{32}}=0.5\rho_{PW} \quad (13)$$

在同时攻击 12 bit 子密钥时，密钥组合为 2^{12} 个，即需要攻击 4 096 个假设密钥。

3 高阶 DPA 攻击实验验证

基于以上分析，对 FPGA 上实现的带变形掩码方案的 DES 算法进行了攻击实验。首先在 DES 运算过程中采集 2 000 条能量迹，在该能量迹上可以清晰地识别出每轮 DES 运算过程，如图 4 所示。

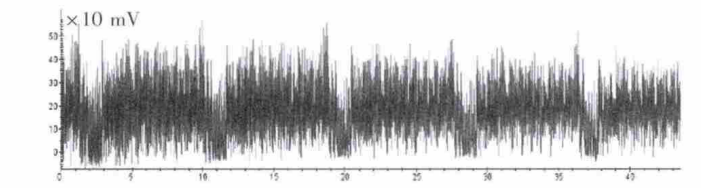

图 4 DES 运算的能量迹

为了找到每轮运算相同操作（例如 S 盒运算）间隔的精确时间，采用模板匹配的方法对能量迹进行处理。其原理是首选选择一段具有代表性的模板，然后用该模板与能量迹进行相关性计算，相关性高的位置将会出现尖峰，如图 5、图 6 所示。

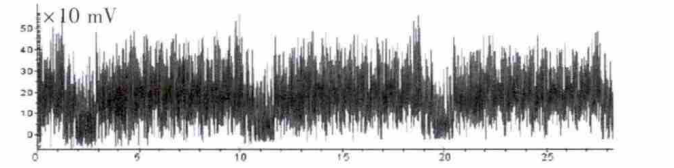

图 5 在某一轮上选择匹配模板

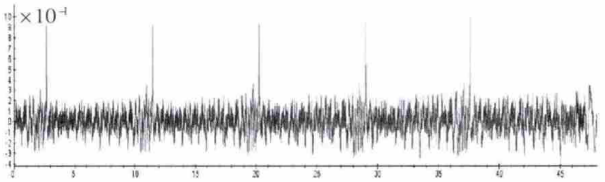

图 6 模板匹配相关性曲线

通过测量模板匹配相关性曲线上相邻尖峰的距离，可以计算出每轮运算的时间间隔。在第一轮运算曲线上找出可能出现的所有间隔为 σ 的两点组合。这些两点组合经过组合函数处理后，形成一条新的曲线。

最后，对组合中间值和新生成的曲线进行相关性运算。在所有 4 096 个相关系数曲线中，峰值最高的曲线所对应的密钥值就是正确的密钥，如图 7 所示。在成功获得 12 bit 密钥后，还需要经过 3 次攻击共获得 48 bit 密钥，剩余的 8 bit 密钥可以通过穷举获得。

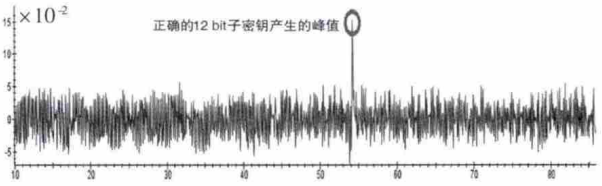

图 7 正确的子密钥产生的相关系数峰值

为了抵抗 DPA 攻击，掩码技术越来越多地被采用。但掩码方案可能受到高阶 DPA 的攻击，因此在设计掩码方案时，需要充分考虑抵抗高阶 DPA 攻击的措施。本文首先介绍了能量泄露模型以及一阶和高阶 DPA 的攻击原理。然后结合变形掩码方案，从理论上证明可以采用二阶 DPA 实施攻击，并且论述了组合函数的选择以及在攻击中提高信噪比的方法。本文最后在 FPGA 上对

(下转第 61 页)

或”阵列的延迟之后输出有效。这额外的延迟 $T_{ex}=\lceil \log_2 d \rceil T_X$。综上所述，总的时钟周期数为 $w+\left\lceil \frac{\lceil \log_2 d \rceil T_X}{T_A+2T_X} \right\rceil$。

表 1 新型字级重序正规基乘法器空间复杂度

#AND	#XOR	#Registers
dm	$2dm$	$(d+2)m+1$

3 性能分析与比较

3.1 性能分析

通过前文分析，对于 GF(2^m)上的模乘运算，该乘法器需要 $w+\left\lceil \frac{\lceil \log_2 d \rceil T_X}{T_A+2T_X} \right\rceil$ 个时钟周期。电路中“与门”个数为 dm，“异或”门个数为 $2dm$，空间复杂度为 dm#AND+$2dm$#XOR，时间复杂度为 T_A+2T_X。将本设计与参考文献[7]中的设计进行比较，电路面积对比如表 2 所示。可以看出，参考文献[7]的设计所占用的电路面积要大于本文中的设计。

表 2 不同字级模乘器之间的下复杂度比较

设计	与门个数	“异或”门个数	运算时间
Namin[7]	$2dm$	$(4d-1)m$	$w(T_{AND}+T_{XOR})+\lceil \log_2 2d \rceil T_{XOR}$
Massey-Omura[8]	$d(2m-1)$	$d(2m-2)$	$w(T_{AND}+(1+\lceil \log_2 m \rceil)T_{XOR})$
本文	dm	$2dm$	$w(T_{AND}+2T_{XOR})+\lceil \log_2 d \rceil T_{XOR}$

在表 2 中，与参考文献[8]中的 Massey-Omura 型乘法器设计相比，本设计采用字级并行结构以后，空间复杂度和时间复杂度均明显降低，这表明电路的时钟频率更高，在花费相同运算时钟周期数的条件下，运算速度更快。

3.2 综合结果

在对 GF(2^{233})上的该型正规基乘法器进行仿真验证后，利用 Synopsys 公司的 Design Compiler 工具在 0.18 μm CMOS 工艺标准单元库下对设计进行综合，表 3 给出了 d=8 时，4.0 ns 约束下的综合报告。

表 3 在 0.18 μm CMOS 工艺标准单元库下的综合结果

#words	关键路径延迟/ns			运算延迟/ns	面积/μm²
	Post Synthesis	Post Place&Route			
8	1.29	1.77		56.64	568 768.540

本文设计了一种支持 II 型最优正规基的字级乘法算法，针对 II 型最优正规基与重序正规基之间的特点，给出了基转换方法，设计了一种新的支持 II 型最优正规基的字级乘法器。根据以上的分析和比较，本文设计的 II 型最优正规基乘法器在运算速度以及面积等方面具有优势，与串行结构的传统正规基乘法器相比，在 GF(2^m)上的乘法运算效率得到显著的提高；与全并行结构的传统正规基乘法器相比，大大减少了电路面积；其关键路径延迟与域元素字长无关，能够满足公钥密码中处理高速性和灵活性的要求。

参考文献

[1] WILSON R M.Optimal normal bases in GF(p^n)[J].Discrete Applied Mathematics, 1988, 89(22): 149-161.

[2] ANSI X9-62.Public key cryptography for the financial service industry-the elliptic curve digital signature algorithm (ECDSA)[S].1999.

[3] ANSI X9-63.Public key cryptography for the financial service industry-the elliptic curve key agreement and apparatus for finite field arithmetic[S].2000.

[4] MULLIN R C, WILSON R M.Optimal normal bases in GF(p^n)[J].Discrete Applied Math, 1989(22)149-161.

[5] GAO S, VANSTONE S.On orders of optimal normal basis generators[J].Math.Computation, 1995, 64(2): 1227-1233.

[6] WU H, HASAN M A, BLAKE I F, et al.Finite field multiplier using redundant representation[J].IEEE Trans. Computers, 2002, 51(11): 1306-1316.

[7] NAMIN A H, Wu Huapeng, AHMADI M.A high speed word level finite field multiplier using reordered normal basis[C].IEEE International Symposium on Circuits and Systems, Seattle, 2008.

[8] MASOLEH A R, HASAN A.Low complexity word-level sequential normal basis multipliers[J].IEEE Transactions on Computers, 2005, 54(2): 98-109.

(收稿日期：2013-03-14)

作者简介：

倪乐，男，1987 年生，硕士研究生，主要研究方向：专用集成电路设计。

(上接第 58 页)

掩码方案的硬件实现进行了攻击实验，并成功获得密钥。

参考文献

[1] KOCHER P, JAFFE J, JUN B.Introduction to differential power analysis and related attacks[A].Cryptography Research Inc., 1998.

[2] KOCHER P, JAE J, JUN B.Differential power analysis[C].In Proceedings of CRYPTO'99, Springer-Verlag, 1999.

[3] MESSERGES T S, DABBISH E A, SLOAN R H, Investigations of power analysis attacks on smartcards[C].In Proceedings of the USENIX Workshop on Smartcard Technology, Chicago, 1999.

[4] AKKAR M L, GIRAUD C.An implementation of DES and AES secure against some attacks[C].In Proceedings of CHES'2001, Springer-Verlag, 2001.

[5] BRIER E, CLAVIER C, OLIVIER F.Correlation power analysis with a leakage model[C].In Cryptographic Hardware and Embedded Systems-CHES 2004, Springer-Verlag, 2004.

[6] MESSERGES T S.Using second-order power analysis to attack DPA resistant software[C].In Proceedings of CHES' 2000, Springer-Verlag, 2000.

(收稿日期：2013-04-24)

作者简介：

赵东艳，女，1971 年生，硕士研究生，高级工程师，主要研究方向：信息安全。

何军，男，1977 年生，硕士研究生，工程师，主要研究方向：信息安全。