DES 芯片抵御高阶差分功耗分析攻击方法研究

李海军† 马光胜 刘晓晓

(哈尔滨工程大学计算机科学与技术学院，哈尔滨 150001)

摘要：分析独特的屏蔽方法及改进方法的不足，提出了逻辑层和算法层相结合抵御高阶差分功耗分析攻击的新方法，并给出芯片半定制设计流程.芯片关键部分电路采用自定义功耗恒定逻辑单元实现，非关键部分电路采用 CMOS 逻辑以减少功耗和面积.整体电路采用独特的屏蔽方法自定义轮实现.结果表明芯片能够抵御高阶差分功耗分析攻击，运算速度与现有方法相当，而所需资源比现有方法少.

关键词：高阶差分功耗分析；独特的屏蔽方法；DES；灵敏放大器型逻辑
PACC：0130Q **EEACC**：1265；2570
中图分类号：TN492 **文献标识码**：A **文章编号**：0253-4177(2008)02-0376-05

1 引言

DES 密码电路和密码算法处理器广泛应用于信息安全领域，如网络加密传输、智能卡等.针对密码芯片的传统攻击方法是用数学手段，通过大量的数学计算来搜寻密钥，攻击难度很大；而且随着密钥长度增加，攻击难度急剧增加.在实际使用中，加密电路运行时会泄露其他信息，如功耗、时间、电磁辐射等，通过观测分析泄漏的信息可能比其他方法更容易获得密钥，即所谓的旁道攻击.差分功耗分析[1](differential power analysis，DPA)研究秘密数据和功耗曲线上一个点的关联，是一种高效、低成本的旁道攻击方法，一般情况下，DPA 是指一阶 DPA.高阶 DPA 是研究秘密数据和功耗曲线上几个点的关联，攻击实施难度增加，但攻击能力增强.DPA 和高阶 DPA 对密码系统构成巨大威胁.

高阶 DPA 中最常见的是二阶 DPA，Messerges[2]第一次报道了用二阶 DPA 成功攻击芯片的例子；Oswald 等人[3]对二阶 DPA 攻击方法进行改进，提出更简单的攻击方法.文献[4]介绍了一种新的二阶 DPA 攻击方法，即重叠攻击.其基本思想是，二阶 DPA 攻击中最困难的是确定所关注的数据运行的准确时刻，而确定 DES 整个轮运行时刻是相对容易的，因此不是去关联能耗轨迹的准确部分，而是直接关联第一轮和最后一轮，这样会降低二阶 DPA 攻击的实施难度.

Tiri[5]提出的灵敏放大器型逻辑(sense amplifier based logic，SABL)运行时功耗几乎恒定，与输入数据及顺序无关，可以用在各种加密电路中提高抵御 DPA 攻击的能力.但是采用 SABL 的芯片功耗和面积增加约一倍，限制了其在移动设备、独立电源设备上的使用.文献[6]采用动态双轨与静态单轨逻辑混合设计，用动态双轨代替静态单轨实现关键模块，来提高抵御 DPA 攻击能力.但是他认为具体替换哪些模块涉及比较复杂的计算，因此没有给出判断关键模块的方法.复制方法[7]、屏蔽方法[8]、变型的屏蔽方法[9]等能够抵御 DPA 攻击，但不能抵御高阶 DPA 攻击[2].

Akkar 等人[4]提出了独特的屏蔽方法(unique masking method，UMM)及改进方法[10]，试图抵御高阶 DPA 攻击 DES(也可应用在 AES 中).文献[11]发现它们并不能抵御高阶 DPA 攻击，在 UMM 改进方法上进一步改进，相对原始 DES 需要额外增加 3 个随机数和 6 个 S 盒.本文提出逻辑层和算法层相结合的新方法，给出半定制设计流程；根据 DES 加密特点，利用 SABL 电路实现 DES 部分电路，结合使用 UMM，使芯片能够抵御任意阶 DPA 攻击.相对原始 DES 只需要额外增加 1 个随机数和 2 个 S 盒，比文献[11]方法所需资源少.

2 功耗分析攻击及抵御方法

2.1 DPA 和高阶 DPA

目前绝大多数集成电路均采用 CMOS 工艺制作，CMOS 门级电路的功耗模型[12]为：

$$P_{\text{total}} = P_{\text{switch}} + P_{\text{short\_circuit}} + P_{\text{leakage}}$$

其中 P_{switch} 为逻辑门翻转引起负载电容充放电导致的功耗，是电路功耗的主要部分；$P_{\text{short\_circuit}}$ 为短路电流导致的功耗；P_{leakage} 为漏泄电流导致的功耗.逻辑门功耗大小与其是否翻转有密切关系，因此电路中运算数据的 0，1 状态与电路的功率信号必然具有一定的相关性，这个特性是 DPA 攻击和高阶 DPA 攻击的物理基础.

DPA 攻击的前提条件是存在中间变量依赖于很少的一部分密钥(一般少于 32bit).如果能够记录芯片运算时功耗变化的特征，结合加密算法的特点，逐一尝试该部分所有可能的密钥就可以得到这部分密钥，进而破

† 通信作者.Email：lllhaijun@tom.com
2007-07-27 收到，2007-10-11 定稿

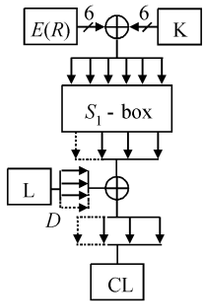

图 1　第一个 S 盒的运算模型

Fig.1　Computation model of the first S-box

解全部密钥.

文献[7]详细介绍了用 DPA 攻击 DES 的方法，高阶 DPA 攻击方法与之类似.高阶 DPA 主要思想是关联几个值来得到重要数据的功耗，攻击需要的数据样本数量和计算量远远大于 DPA，这导致高阶 DPA 攻击难度增加，限制了其应用.在实施攻击过程中，攻击对象是依赖少于 32bit 密钥的数据；依赖高于 32bit 密钥的数据，对其实施攻击代价太大，失去了旁道攻击的意义.图 1 是第一个 S 盒的运算模型，其中虚线代表的值与选择函数 D 的值有关联.

2.2　UMM 及攻击它的方法

UMM 方法大致可以分为 2 个步骤：

第 1 步：得到屏蔽的轮

产生一个 32bit 的随机数 α，基于原始 DES 中 S 盒函数，自定义 2 个 S 盒 $\tilde{S}_1$ 和 $\tilde{S}_2$ 如下：

$$\forall x\in\{0,1\}^{48},\tilde{S}_1(x)=S(x\oplus E(\alpha))$$

$$\forall x\in\{0,1\}^{48},\tilde{S}_2(x)=S(x)\oplus P^{-1}(\alpha)$$

这里　E 是扩展变换；P^{-1} 是 S 盒之后的逆置换.

定义 f_{Ki}，$\tilde{f}_{1,Ki}$ 和 $\tilde{f}_{2,Ki}$ 函数如下：

f_{Ki} 函数由扩展变换 E，第 i 轮子密码 K_i，S 盒以及 P 置换构成；将 f_{Ki} 函数中 S 盒分别用 $\tilde{S}_1$ 和 $\tilde{S}_2$ 代替得到 $\tilde{f}_{1,Ki}$ 和 $\tilde{f}_{2,Ki}$.可以看出 $\tilde{f}_{1,Ki}$ 是从屏蔽过的值得到没屏蔽的值，$\tilde{f}_{2,Ki}$ 则从没屏蔽的值得到屏蔽过的值.用 f_{Ki}，$\tilde{f}_{1,Ki}$ 和 $\tilde{f}_{2,Ki}$ 函数可以得到屏蔽或者没屏蔽的 5 种类型的轮：

A 类：输入的左右两部分都没屏蔽，函数是 f_{Ki} 函数，因此输出的左右两部分是没屏蔽的值.

B 类：输入的左右两部分都没屏蔽，但函数是 $\tilde{f}_{2,Ki}$ 函数，因此输出的左边部分是没屏蔽的值，而右边部分是屏蔽的值.

C 类：输入的左边部分没屏蔽，而右边部分屏蔽，函数是 $\tilde{f}_{1,Ki}$ 函数，因此输出的左边部分是屏蔽的值，而右边部分是没屏蔽的值.

D 类：输入的左边部分屏蔽，而右边部分没屏蔽，函数是 f_{Ki} 函数，因此输出的左边部分是没屏蔽的值，而右边部分是屏蔽的值.

E 类：输入的左边部分屏蔽，而右边部分没屏蔽，函数是 $\tilde{f}_{2,Ki}$ 函数，因此输出的左右两部分都是没屏蔽的值.

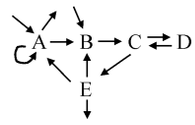

图 2　自定义 5 种类型轮的合法序列

Fig.2　Valid sequence for five kinds of user-defined rounds

第 2 步：用屏蔽的轮组成 DES

DES 的轮序列由图 2 所示的有限状态自动机构成.为了抵御 DPA 攻击，所有依赖少于 36bit 密钥的值都用随机数进行屏蔽，这进一步限制了轮序列：最前 3 轮必须是 BCD 或 BCE，最后 3 轮必须是 BCE 或 DCE.

将第 3 至 14 轮用不同类型的轮实现，如 IP－BC－DCDCEBCDCDCD－CE－IP^{-1} 是一个合法的轮序列，IP 和 IP^{-1} 分别表示初始置换和逆初始置换.

采用 UMM 方法实现的 DES 第 2 轮 $\tilde{S}$ 盒输出是：$S(E(P(S(K_1\oplus E(\mathrm{IP}(M)_{32-63})))\oplus\mathrm{IP}(M)_{0-31}\oplus\alpha_1)\oplus K_2\oplus E(\alpha_1))$，由于扩展变换 E 是线性函数，将其展开得到 $S(E(P(S(K_1\oplus E(\mathrm{IP}(M)_{32-63}))))\oplus E(\mathrm{IP}(M)_{0-31}\oplus E(\alpha_1)\oplus K_2\oplus E(\alpha_1))$，两个 $E(\alpha_1)$ 异或消除后得到 $S(E(P(S(K_1\oplus E(\mathrm{IP}(M)_{32-63}))))\oplus E(\mathrm{IP}(M)_{0-31})\oplus K_2)$，该轮 $\tilde{S}$ 盒输出没有随机数屏蔽，而且与消息的左边部分异或后仍然没屏蔽，文献[10]给出了用选择明文攻击它的方法.其改进方法[10]定义一个 $\tilde{f}_{3,Ki}$ 函数，修改 $\tilde{S}_3$ 使得 $\forall x\in\{0,1\}^{48}:\tilde{S}_3(x\oplus E(\alpha_1))=S(x)\oplus P^{-1}(\alpha_1)$，改进后的第 2 轮 $\tilde{S}$ 输出为：

$S(E(P(S(K_1\oplus E(\mathrm{IP}(M)_{32-63})))\oplus\mathrm{IP}(M)_{0-31}\oplus\alpha_1)\oplus K_2)$

同前面类似，将 E 展开可以得到：

$S(E(P(S(K_1\oplus E(\mathrm{IP}(M)_{32-63}))))\oplus E(\mathrm{IP}(M)_{0-31})\oplus E(\alpha_1)\oplus K_2)$

结合 $\tilde{S}_3$ 的定义，得到第 2 轮 $\tilde{S}$ 输出值为：

$$S(E(P(S(K_1\oplus E(\mathrm{IP}(M)_{32-63}))))\oplus E(\mathrm{IP}(M)_{0-31})\oplus K_2)\oplus P^{-1}(\alpha_1)\quad(1)$$

输出值(1)中每次加密都将有一个不同的随机值 $P^{-1}(\alpha_1)$，由于它对攻击者是未知的，攻击者不能正确地分组功耗信息，因此攻击不能成功.

文献[11]发现上面的改进方法中，DES 的第 1，2 轮的 $\tilde{S}$ 盒输出是用相同随机数屏蔽的，这个特点是其攻击方法的基础，可以用下面几步实现攻击：

第 1 步：第 1 轮 $\tilde{S}$ 盒的输出：

$$S(K_1\oplus E(\mathrm{IP}(M)_{32-63}))\oplus P^{-1}(\alpha_1)\quad(2)$$

第 2 步：第 2 轮 $\tilde{S}$ 盒的输出：

$S(E(P(S(K_1\oplus E(\mathrm{IP}(M)_{32-63}))))\oplus E(\mathrm{IP}(M)_{0-31})\oplus K_2)\oplus P^{-1}(\alpha_1)$

第 3 步：通过异或第 1，2 轮的 $\tilde{S}$ 盒输出(即 XOR 值(1)和值(2))得到：

$$S(E(P(S(K_1 \oplus E(\mathrm{IP}(M)_{32-63}))))\oplus E(\mathrm{IP}(M)_{0-31})\oplus K_2)\oplus S(K_1\oplus E(\mathrm{IP}(M)_{32-63})) \quad (3)$$

随机值 $P^{-1}(\alpha_1)$在(3)式中消失了,可以用选择明文攻击[11]:固定 $\mathrm{IP}(M)_{32-63}$为一个任意的随机值,让 $\mathrm{IP}(M)_{0-31}$随机输入,可以得到(3)式中 $E(P(S(K_1\oplus E(\mathrm{IP}(M)_{32-63}))))\oplus K_2$ 的值,通过足够多的样本,再用类似于重叠攻击的方法进行攻击.因此文献[10]的改进方法仍然不能抵御高阶 DPA 攻击.

3 改进的 DES 抵御高阶 DPA 攻击方法

文献[11]通过异或第 1,2 轮的 $\tilde{S}$ 盒输出,消除 UMM 方法用来对这 2 轮进行屏蔽的随机值,使屏蔽作用失效,再用选择明文输入,采用类似重叠攻击的方法攻击这 2 轮,进而攻击整个 DES.该方法可以用来攻击第 15,16 轮,但这要求 DES 输出的指定部分相同,只保留输出指定部分相同的样本,这需要极大的样本数,在实际中不可行,因此攻击第 15,16 轮只有理论意义,没有实际意义.这 4 轮泄露的能耗特征容易被攻击,UMM 方法没有很好地屏蔽,它们是抵御高阶 DPA 攻击的薄弱环节.由于 UMM 轮的独特性,DES 中第 3 至 14 轮有多种合法轮序列,可以每次加密后改变轮序列.轮序列不同,则每轮屏蔽类型不同,攻击者不能关联功耗曲线上多个点,也就不能分组功耗曲线,高阶 DPA 攻击失效.文献[11]从算法层考虑提出抵御方法,认为屏蔽 16 轮抵御高阶 DPA 需要满足 5 个条件.这些条件本质上是要求对轮进行有效屏蔽,使得攻击者不能消除随机数.

我们认为可以结合使用其他方法来保护关键的第 1,2,15,16 轮,而不仅仅是 16 轮都用屏蔽方法.将这 4 轮用功耗恒定的 SABL 逻辑门来实现,提高抵御重叠攻击的能力,使文献[11]提出的攻击这 2 轮的方法失效,这样就不需要满足他提出的 5 个条件.结合 UMM 方法,将第 3 至 14 轮用不同合法轮序列实现,整个算法只需用 1 个随机数进行屏蔽.

设计过程大致分为以下几步:设计功耗恒定标准逻辑单元;用得到的逻辑单元构建功耗平衡的 DES 轮;采用 UMM 方法定义 5 种类型的轮;按照合法的轮序列构建整体 DES 芯片;对芯片进行功耗模拟,证实抵御功耗攻击的能力.

3.1 功耗平衡的 DES 轮

S 盒采用 SABL 逻辑门实现的 DES 轮记为 SABL_S,其功耗平衡可以提高抵御 DPA 攻击及重叠攻击的能力.从晶体管开始设计,定制功耗恒定的逻辑门电路,用此门电路实现关键的 4 轮,得到功耗平衡的轮.图 1 是 DES 中第 16 轮的第一个 S 盒示意图,其他模块的电流变化对 DPA 攻击影响不大,不予考虑.

SABL 逻辑门是动态和差分逻辑的组合.当时钟信号下降为低电平后,电路开始预充电,双轨输出都被预充到高电平;当时钟信号上升为高电平后,电路处于求值阶段,不管输入什么信号,双轨输出一个维持高电平,一个降为低电平,保持功耗恒定.相同逻辑功能的 SABL 电路比 CMOS 电路的晶体管数量多,晶体管数量增多导致电路面积和功耗增加,SABL 是以此为代价得到功耗恒定的.我们基于 SABL 设计功耗恒定的逻辑门标准单元库:使用 CosmosSE 设计逻辑图;用 Hspice 模拟时调整晶体管的长宽比,确定一种合适的长宽比;将确定晶体管长宽比的逻辑 Spice 网表用工具生成 GDSII 格式的版图文件,提取版图中的各种寄生参数;基于这些参数,用 Hspice 模拟得到标准单元的功能、传输延迟、上升下降时间等关键参数,形成标准单元库.

以每个周期来计算能耗,文献[5]提出了功耗变化幅度的计算公式,标准功耗偏差(normalized energy deviation,NED)是最大和最小能耗之间的差与最大能耗的比值,即:

$$\mathrm{NED}=\frac{\mathrm{Max(energy/cycle)}-\mathrm{Min(energy/cycle)}}{\mathrm{Max(energy/cycle)}}$$

$\mathrm{NED}\in[0,1]$,可以衡量抵御功耗攻击的能力.该值越小,抵御功耗攻击能力越强,反之亦然.将 S 盒用 SABL 逻辑构成,对 S 盒的 Spice 网表进行模拟得到 NED 值为 2.32%.

3.2 采用 UMM 保护的 DES 轮

S 盒采用 CMOS 逻辑门实现的 DES 轮记为 CMOS_S,其功耗与输入数据、输入顺序有关联会被 DPA 攻击,需要结合屏蔽方法来保护.由于 S 盒是一个非线性函数,屏蔽后的数据直接经过 S 盒后将不能再还原,必须在进入 S 盒之前将数据进行还原或者修改 S 盒.本文与 UMM 方法类似,对 S 盒进行修改.产生 1 个随机数,自定义 2 个额外的 $\tilde{S}$ 盒,用修改过的 $\tilde{S}$ 盒替代原始 S 盒,得到 5 种类型轮,通过这些轮组成不同的轮序列.第 3 至 14 轮有很多合法的轮序列,如 IP-BC-DCDCEBCDCDCD-CE-IP^{-1} 和 IP-BC-DCDCDCEBCDCD-CE-IP^{-1}等,IP 和 IP^{-1}分别表示初始置换和逆初始置换.在每次完成加密后改变合法轮序列,达到抵御高阶 DPA 攻击的目的.

3.3 DES 芯片的硬件实现

由于电路采用不同类型的逻辑构成,传统的设计流程不完全适用,我们提出采用半定制设计流程,在满足设计要求情况下,充分利用现有工具提高设计速度.考虑到 DES 芯片运算速度、面积和成本的约束,将部分模块复用.我们以合法序列 IP-BCDCDCEBCDCDCDCE-IP^{-1}为例,将第 1,2,15,16 轮用 SABL 逻辑实现,第 3 至 14 轮用 CMOS 逻辑实现,轮序列记为 IP-$(\mathrm{BC})_{\mathrm{SABL_S}}$ $(\mathrm{DCDCEBCDCDCD})_{\mathrm{CMOS\_S}}$ $(\mathrm{CE})_{\mathrm{SABL\_S}}$-$\mathrm{IP}^{-1}$,$(\mathrm{BC})_{\mathrm{SABL_S}}$表示 UMM 方法中的 B 类和 C 类用 SABL 逻辑实现,其他与此类似.图 3 是实现 DES 的关键模块电路结构图,省略了其他辅助模块.芯片设计流程与基于 CMOS 标准单元库的设计流程大体相同,在综合仿真阶段用的库文件是自定义功耗恒定的逻辑单

表 1　不同方法实现 DES 所需资源比较

Table 1　Comparison of required resources in implementing DES with different methods

实现 DES 的方法	随机数个数	额外 S 盒个数	实现 DES 采用的逻辑（无模块复用时）	加密一次时间（有模块复用时）	是否能够抵御高阶 DPA 攻击
UMM[4]	2	2	16 轮 CMOS	38ms	不能
改进的 UMM[10]	2	3	16 轮 CMOS	–	不能
参考文献[11]的方法	3	6	16 轮 CMOS	67ms(最坏情况)	能够
本文的方法	1	2	4 轮 SABL,12 轮 CMOS	约 70ms	能够

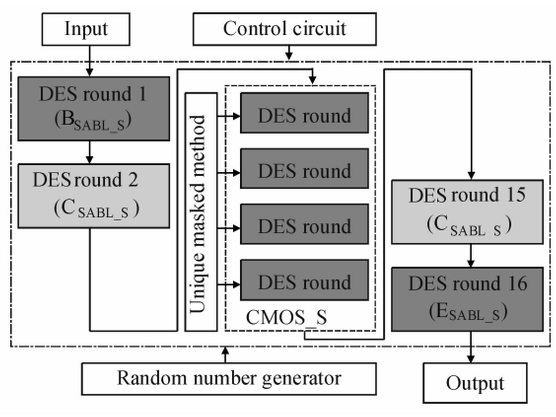

图 3　综合方法实现 DES 结构图

Fig.3　DES structure implemented by combination approach

元库.在后端设计上,用自动布局布线工具对其进行布局布线.我们对加密模块进行仿真,能够实现标准 DES 的加/解密功能.对芯片 Spice 网表进行功耗模拟,得到的功耗样本统计显示功耗曲线差异较小,达到预定设计目标.在流片前用软件模拟检验它的防御能力的好处是减少流片次数,缩短设计周期和降低成本.

4　抵御高阶 DPA 攻击验证及性能分析

本文用 SABL 逻辑实现功耗恒定的标准单元库,用该单元实现 DES 第 1,2 轮(还有第 15,16 轮),其功耗变化幅度几乎为 0.不管 UMM 方法中第二轮 $\bar{S}$ 盒输出有没有被屏蔽,或者第 1,2 轮是否用相同的随机数屏蔽,它都可以抵御功耗攻击.提高了这 4 轮抵御选择明文及重叠攻击的能力,弥补 UMM 的薄弱环节,使文献[11]提出的攻击失效.

实现抵御高阶 DPA 攻击的 DES 时,UMM 方法需 2 个额外 S 盒,在 ST19 元件工作频率为 10MHz 时,实现一次加密时间是 38ms[4];文献[11]需 6 个额外的 S 盒,其估算一次加密时间是 67ms.本文方法需 2 个额外的 S 盒,在 10MHz 工作频率下,加密一次约耗时 70ms.表 1 对比了几种方法实现 DES 所需的资源.

文献[5]给出了分别用 SABL 和 CMOS 实现 S_9-box 芯片的功耗和面积比较,前者分别是后者的 1.91 倍和 1.80 倍.在不进行模块复用,不考虑其他次要因素的情况下,假设采用 CMOS 结构实现 DES 一轮的功耗和面积分别是 p 和 a,则整个 DES 芯片功耗和面积分别是 $16p$ 和 $16a$;基于 SABL 分别是 $30.56p$ 和 $28.8a$;本文中 4 轮用 SABL 实现,12 轮用 CMOS 实现,功耗和面积分别是 $19.64p$ 和 $19.2a$.表 2 列出了不同逻辑门实现 DES 的功耗和面积.

表 2　不同逻辑门实现 DES 的功耗和面积比较

Table 2　Comparison of power consuming and area in implementing DES with different logic gates

实现 DES 的逻辑门	功耗	面积	是否能够抵御 DPA 攻击	是否能够抵御高阶 DPA 攻击
CMOS	$16p$	$16a$	不能	不能
SABL	$30.56p$	$28.8a$	能够	不能
本文的方法（CMOS 和 SABL）	$19.64p$	$19.2a$	能够	能够
本文的方法/SABL	64.27%	66.67%	–	–

5　结论

本文提出逻辑层和算法层相结合设计 DES 芯片的方法,指出 DES 的第 1,2,15,16 轮是抵御功耗攻击的关键轮;提出芯片半定制设计流程,用 SABL 生成功耗恒定逻辑标准单元库,用该单元实现关键轮弥补 UMM 的薄弱环节;结合 UMM 使芯片能够抵御高阶 DPA 攻击.芯片在功耗、面积等指标上比将 16 轮全部屏蔽的现有方法好,运算速度相当.本文方法可以进一步采用硬件复用,但会增加延迟,降低运算速度.随后我们将进一步研究将 UMM 应用在 AES 时,是否同样会被文献[11]提出的方法攻击.如果能够被攻击,将考虑用 SABL 实现部分电路的方法来抵御,并考虑如何减小自定义 S 盒所需内存.

参考文献

[1] Kocher P,Jaffe J,Jun B. Differential power analysis. Proceedings of Advances in Cryptology(CRYPTO'99),1999:388

[2] Messerges T S. Using second-order power analysis to attack DPA resistant software. CHES,2000:238

[3] Oswald E,Mangard S,Herbst C,et al. Practical second-order DPA attacks for masked smart card implementations of block ciphers. CT-RSA,2006:192

[4] Akkar M L,Goubin L. A generic protection against high-order differential power analysis. Fast Software Encryption(FSE2003),2003:192

[5] Tiri K, Akmal M, Verbauwhede I. A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards. Proc of the 28th European Solid-State Circuits Conf,2002:403

[6] Tong Yuanman,Wang Zhiying,Dai Kui,et al. Semi-custom design flow:Protecting security IC's against power analysis based on dy-

namic dual-rail logic. Journal of Chinese Computer Systems, 2007, 28(5): 935(in Chinese)[童元满, 王志英, 戴葵, 等. 基于动态双轨逻辑的抗功耗攻击安全芯片半定制设计流程. 小型微型计算机系统, 2007, 28(5): 935]

[7] Goubin L, Patarin J. DES and differential power analysis: the duplication method. CHES, 1999: 158

[8] Messerges T S. Securing the AES finalists against power analysis attacks. Fast Software Encryption (FSE2000), 2000: 150

[9] Akkar M L, Giraud C. An implementation of DES and AES, Secure against Some Attacks. CHES, 2001: 309

[10] Akkar M L, Bevan R, Goubin L. Two power analysis attacks against one-mask methods. Fast Software Encryption (FSE2004), 2004: 332

[11] Lv Jiqiang, Han Yongfei. Enhanced DES implementation secure against high-order differential power analysis in smartcards. Australasian Conference on Information Security and Privacy (ACISP2005), 2005: 195

[12] Han Jun, Zeng Xiaoyang, Tang Ting'ao. VLSI design of anti-attack DES circuits. Chinese Journal of Semiconductors, 2005, 26(8): 1646(in Chinese)[韩军, 曾晓洋, 汤庭鳌. DES 密码电路的抗差分功耗分析设计. 半导体学报, 2005, 26(8): 1646]

An Approach to Resisting High-Order Differential Power Analysis Attacks on DES Chips

Li Haijun†, Ma Guangsheng, and Liu Xiaoxiao

(*College of Computer Science and Technology, Harbin Engineering University, Harbin* 150001, *China*)

Abstract: After analyzing the disadvantage of the unique masking method (UMM) and its improvements, a new approach combining the logic level with the algorithm level is presented to resist high-order differential power analysis (DPA) attacks, and the semi-custom design flow is also given. The critical circuits are implemented with user-defined constant power consuming logic cells, while the non-critical circuits are implemented with CMOS logic to reduce power consumption and area. The whole circuit is implemented with the UMM self-define the round. Experimental results show that our chip can resist high-order DPA attacks. The operation speed is comparable with that by the present methods, but the resource requirements are lower.

Key words: high-order differential power analysis; unique masking method; DES; sense amplifier based logic
PACC: 0130Q **EEACC**: 1265; 2570
Article ID: 0253-4177(2008)02-0376-05

† Corresponding author. Email: lllhaijun@tom.com
Received 27 July 2007, revised manuscript received 11 October 2007