哈尔滨工程大学

博士学位论文

加密芯片的旁道攻击防御对策研究

姓名：李海军

申请学位级别：博士

专业：计算机应用技术

指导教师：马光胜

20081101

摘　要

功耗攻击方法是得到广泛重视和应用的一种旁道攻击方法，它观测加密芯片运行时的功耗变化特征，研究处理数据与功耗之间的相关性，根据相关性推算出芯片内部存储的密钥。功耗攻击方法实施简单，攻击能力强，具有通用性，与具体加密算法无关，能够攻击各种加密算法的芯片。差分功耗分析（Differential Power Analysis, DPA）和高阶差分功耗分析（High Order Differential Power Analysis, H-O DPA）攻击能力更强，而且随着研究的深入，实施攻击方法越来越成熟，攻击成本下降，对加密芯片构成极大威胁。有些针对特定加密算法进行改进的攻击方法，其攻击效果更好。

本论文主要针对功耗分析技术的特点及关键技术，特别是DPA和高阶DPA技术进行研究，提出具体的改进防御方法，增强加密芯片防御DPA的能力，并进行加密芯片的设计和仿真。对新出现的专门针对具体加密算法的攻击方法，也进行了研究并提出相应的防御方法。完成的主要研究工作如下：

1）提出修改AES算法的防御方法。引入随机化方法和变形屏蔽方法（Transformed Masking Method, TMM）修改AES算法，同时将AES算法中$GF(2^8)$求逆运算的部分用简单动态差分逻辑构建，使AES芯片能够防御零值攻击。安全性分析表明，攻击新的方法所需的样本数是标准二阶DPA攻击的$(16+4*n)^2$倍，这使攻击变得不可行，仿真表明可以防御零值攻击。

2）对采用屏蔽方法的DES芯片提出改进的屏蔽方法。在数据进入S盒之前不恢复密钥，而是修改S盒，即能够保护密钥，又使得数据在经过S盒变换后能够消除屏蔽。DES算法中同时存在异或屏蔽和加法屏蔽，引入两者之间相互安全转换的方法，使得算法中的敏感数据不以明文出现，能够完全屏蔽。分析表明可以防御关联攻击、重叠攻击等新的攻击方法。

3）针对DES加密系统提出采用算法层和逻辑层组合的方法改进独特屏蔽方法（Unique Masking Method, UMM）；研究灵敏放大器型逻辑（Sense Amplifier Based Logic, SABL）特性，设计功耗平衡SABL单元库，半定制设计流程，并指出用SABL实现S盒的原因。对其安全性分析和仿真实验表明可以防御高阶DPA攻击。

4）设计能够防御高阶DPA攻击的DES芯片。修改原始S盒，增加1个随机数和2组S盒。采用SABL实现DES芯片关键部分模块；采用CMOS实现非关键部分模块，最后构成整体DES芯片。设计实现芯片时考虑智能卡的限制，在一些性能指标上进行折中，采用部分流水结构。对其进行性能仿真并与现有芯片进行分析比较，芯片能够实现加解密，提高防御高阶DPA攻击的能力，比以前的方法节省资源。

关键词：信息安全；加密算法；加密硬件；功耗分析；屏蔽方法；功耗平衡

Abstract

Power analysis method is a side channel attack method which got widely attention and application, it observes the power variation characteristic when encryption chip running, research the correlation of processing data and power consuming, to reason the Key stored in the chip according to correlation. For our approach is easy and the attack ability is strong, this approach is widely adopted. It can attack the chip with all kinds of encryption algorithm, not constrained by a specific algorithm. Differential power analysis (DPA) and high order DPA (H-O DPA) attack ability is stronger, with the development of research, the implementation approach is mature, the cost reduced dramatically, they seriously threaten encryption chip. There are many improved power attack approach aim at the specifically encryption algorithm and the attack effect is better.

Our thesis aimed at the characteristic of power attack technology and critical technology, especially DPA and high order DPA, to proposes improved specify defend approach, to enhance encryption chip defeat DPA, to design the encryption chip and simulation. To research the defend approach according to new attack approach, our main works are as follows:

1) Propose defend method which modified AES algorithm. Introduce the random method and Transformed Masking Method (TMM) to modify AES algorithm, to implement with the inverse operation of $GF(2^8)$ in the AES algorithm with the Simple Dynamic Differential Logic (SDDL) logic. The analysis indicates that success attack need $(16+4*n)^2$ times trace than the standard DPA, this is infeasible. The simulation experiment indicates that our approach can defend the zero value attack.

2) Propose an improved method with masking approach DES encryption chip, to modify the S box instead of restoring the key before proceeding data input s-box, it can protect key and to eliminate data masking after the transformation of S box. There exist XOR masking and Addition masking operation in the DES algorithm, we implement the approach to transform in the XOR masking and

Addition masking operation, the sensitive data will not appear in the cipher text and is completely masked. The simulation result indicates it can defend the correlation attack, superposition attack and so on

3) Propose improved Unique Masking Method (UMM) algorithm which combines algorithm level and logic level method aiming at DES encryption system; Research the characteristic of Sense Amplifier Based Logic (SABL), design power consuming balance SABL cell library, semi-custom design flow and point out the reason to implement S box with SABL. The security analysis and simulation experiment shows our approach can defend the high-order DPA attack.

4) Design the DES chip which can defend high order DPA attack. To modify the S box, add one random number and two groups of S boxes. To achieve the DES chip critical module with SABL, non-critical module is implemented with CMOS, then construct the whole DES chip finally. To tradeoff some performance index in the implementation process consider the restriction of smartcard, a part segment pipeline was used in its structure. To implement simulation analysis with the performance and comparison with the chip in existence, it shows that the chip can achieve encryption and decryption. The new approach improved the ability of defending high order DPA attack, reduced the resource consuming in the mean time.

KeyWords: information security; encryption algorithm; encryption hardware; power analysis; masking method; power balance

哈尔滨工程大学
学位论文原创性声明

本人郑重声明：本论文的所有工作，是在导师的指导下，由作者本人独立完成的。有关观点、方法、数据和文献的引用已在文中指出，并与参考文献相对应。除文中已注明引用的内容外，本论文不包含任何其他个人或集体已经公开发表的作品成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律结果由本人承担。

作者（签字）：李海军

日期：2008年 11月 9日

第1章 绪 论

1.1 课题的研究背景及意义

1.1.1 课题背景

近年来，随着信息化进程不断推进，信息系统在政府和大型行业、企业组织中得到了广泛应用，信息系统安全管理已经成为政府、行业、企业管理关键的部分，研究可靠的信息安全技术受到全世界的普遍关注。信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。信息安全本身包括的范围很大，大到国家军事政治等机密安全，小范围的包括如防范商业企业机密泄露，个人信息的泄露等。信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名，信息认证，数据加密等），直至安全系统，其中任何一个安全漏洞便可以威胁全局安全。信息安全的实现目标：

1）真实性：对信息的来源进行判断，能对伪造来源的信息予以鉴别。

2）保密性：保证机密信息不被窃听，或窃听者不能了解信息的真实含义。

3）完整性：保证数据的一致性，防止数据被非法用户篡改。

4）可用性：保证合法用户对信息和资源的使用不会被不正当地拒绝。

5）不可抵赖性：建立有效的责任机制，防止用户否认其行为。

6）可控制性：对信息的传播及内容具有控制能力。

7）可审查性：对出现的网络安全问题提供调查的依据和手段。

作为信息安全关键技术的密码学是一门关于加密与破译技术的学科，它可以分为密码编码学（Cryptography）与密码分析学（Cryptanalysis）两部分。密码编码学主要研究密码算法与使信息得到保护的技术；而密码分析学则恰恰相反，它是一门破译密文的科学与技术，要非法获得或破坏明文[1-3]。

现代密码学大致可被区分为数个领域，研究内容主要在分组密码（Block Cipher）与流密码（Stream Cipher）及其应用。

1）分组密码取用明文的一个区块和密钥，输出相同大小的密文区块。由于信息通常比单一区块还长，因此有了各种方式将连续的区块编织在一起。数据加密标准（Data Encryption Standard, DES）和高级加密标准（Advanced Encryption Standard, AES）是美国联邦政府核定的分组密码标准，尽管AES将取代DES，从标准上废除DES，目前DES依然很流行（Triple-DES变形仍然相当安全），在非常多的应用上使用，从自动交易机、电子邮件到远端存取。

2）流密码，相对于区块加密，制造一段任意长的钥匙原料，与明文依位元或字符结合，有点类似一次垫（one-time pad）。输出的串流根据加密时的内部状态而定。在一些流密码上由钥匙控制状态的变化，RC4是有名的流密码。

公开密钥密码体系，简称公钥密码体系，又称非对称密钥密码体系，相对于对称密钥密码体系，最大的特点在于加密和解密使用不同的密钥。公开密钥的算法大多基于计算复杂度上的难题，通常来自于数论。例如RSA源于整数因子分解问题；DSA源于离散对数问题。近年发展快速的椭圆曲线密码学则基于椭圆曲线相关的数学难题，与离散对数相当。由于这些底层的问题多涉及模数乘法或指数运算，相对于分组密码需要更多计算资源。

加密技术可使一些重要数据存储在不安全的计算机上，或在不安全的信道上传送，只有持有合法密钥的一方才可以获得明文。密码技术保护的现代系统的安全性主要取决于对密钥的保护，而不是对算法和硬件本身的保护，其密码算法的安全性完全取决于密钥的安全。加密算法的物理实现称作密码模块或密码设备，它包括专用集成电路实现与软件实现两种。

由于计算机运算速度的不断提高，各种攻击密码算法的方法被提出，密码算法面临着新的挑战，信息安全已经成为未来信息技术中需要研究的关键问题之一。研究人员针对这些新挑战提出很多新的密码体制，如量子密码、DNA密码、混沌理论等，这些密码新技术正处于探索之中[4]。

加密系统设计人员通常认为秘密信息是在一个封闭可信赖的计算环境中进行处理，因此都将注意力集中在协议和数学算法的安全性上[5]，对应的破译方法也主要是针对这方面。差分分析[6]和线性分析[7]是分组密码分析中最主要的两种方法[8]，随着分组密码设计理论的发展，越来越多的新算法开始抵抗传统的分析方法，与此同时越来越多的分析工具被分析学家们所使用，比如文献[9-14]提出的方法等等。不幸的是，现实中的计算操作并不一定是在安全可靠的环境

中，在实际使用中加密电路运行时会泄露其它信息，泄露的信息可以被利用来攻击加密电路[15]。人们开始注意到仅仅考虑加密算法是不足以确保数据安全性的，还必须要考虑实现加密算法硬件的安全性。

因此密码芯片的设计中就需要考虑实现安全问题，密码芯片的实现安全问题可描述为：作为密码算法的物理载体，密码芯片能够正确实现算法功能的同时，算法不可被外界访问的中间结果和内部保密数据，以及外界无法获得的其它数据信息不会通过物理途径泄露，它们的内容无法被危害算法安全性地篡改。保证密码算法的实现安全的实现方案称为“安全实现”。存在实现安全问题的密码芯片包括那些内部存有密钥等数据的芯片和其所处系统中存有密钥，要使用这些密钥执行加/解密运算的芯片。

1.1.2 课题意义

DES、AES、RSA密码电路和密码算法处理器广泛应用于信息安全领域，如网络加密传输和智能卡等。针对密码芯片（智能卡）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。而当前主流的加密算法，如对称加密算法DES和AES，非对称加密算法RSA等等在数学上是安全可靠的。因此攻击难度很大，而且随着密钥长度增加攻击难度急剧增加。实际上信息系统任何一个环节的弱点都可能成为被攻击的途径。智能卡在输入信息和密钥进行处理的过程中，会泄漏一些信息，如功耗、时间、电磁辐射等等，如图1.1所示。旁道信息是指当密码模块运算密码算法时，密码模块外部可观察的物理信息。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。旁道攻击方法除了需要芯片输入输出结果，还要用到模块的一些旁道信息。

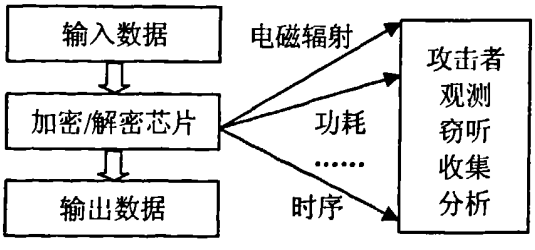

图1.1 旁道信息泄露

Figure1.1 Side channel information leaking

实施旁道攻击代价低廉，并且相当有效，所以它对密码芯片的安全产生了

极大的危害。对信息安全人员来说除了考虑加密算法本身的安全性，还必须考虑数据在硬件中进行加密和存储操作时可能受到的旁道攻击，这需要从系统的角度来考虑数据的安全性，由此对硬件提出了安全性要求。

1.2 智能卡安全工作原理

IC 卡是集成电路卡（Integrated Circuit Card）的英文简称，也称之为智能卡、智慧卡、微芯片卡等。将一个专用的集成电路芯片镶嵌于符合 ISO 7816 标准的 PVC（或 ABS 等）塑料基片中，封装成外形与磁卡类似的卡片形式即制成一张 IC 卡。IC 卡硬件主要由 CPU、ROM、RAM、EEPROM、输入输出接口、安全逻辑、加密解密运算协处理器等一系列功能部件组成。目前智能 IC 卡的 CPU 以微处理器为主，存储器的容量比较小，其中 RAM 容量很小，为 1k 字节左右，ROM 容量为 20k 字节左右，EEPROM 容量为 10k 字节左右。

当前智能卡的应用已经遍布世界各地，广泛应用于电子货币，数字签名，身份认证和信息安全等领域。智能卡被用来存储和在加密系统中应用密钥，在一个简单的应用中，智能卡可能通过一个邀请-响应协议提供授权。在这个协议中，一个外部设备称为读卡器，将要求智能卡加密一个随机数。智能卡就能够用它自己的密钥来加密这个随机数并且给出响应。然后读卡器和智能卡共享相同的密钥，读卡器能够检测响应并且验证智能卡是否被授权。

读卡器向智能卡（以读写卡为例，主要是 M1 卡，也叫 MifareOne 卡）发一组固定频率的电磁波，卡片内有一个 LC 串联谐振电路，其频率与读卡器发射的频率相同。在电磁波的激励下，LC 谐振电路产生共振，从而使电容内有了电荷。在这个电容的另一端，接有一个单向导通的电子泵，将电容内的电荷送到另一个电容内储存。当所积累的电荷达到一定电压（2V）时，此电容可做为电源为其它电路提供工作电压，将卡内数据发射出去或接取读卡器的数据。

合法可靠的读卡器拥有智能卡的密钥的一个备份，因此这些读卡器能够验证响应的结果，不合法的读卡器不能知道智能卡的密钥。然而当智能卡加密随机数时，泄漏消耗能量的信息，使得不合法的读卡器可能根据这些信息探知智能卡的密钥，成功获得密码后就可以伪造智能卡。智能卡的发行者和使用者都期望能够采取防御措施，使得能耗信息不能揭示密钥。

1.3 攻击智能卡的常规方法

攻击智能卡安全系统的方法可分为两大类：1）对智能卡安全系统所采用的密码算法的数学性质进行密码分析，前面介绍的各种数学分析方法即是；2）对智能卡硬件本身进行攻击。根据攻击时是否对智能卡硬件本身进行破坏又可以分为破坏性攻击和非破坏性攻击两类。

破坏性攻击是破坏芯片的正常工作，采用物理方法解剖芯片。用特殊技术和方法将集成芯片从智能卡中取出，芯片露出来后，使用高精度的仪器设备对芯片内部的电路进行分析，用针探测或者用聚集离子束系统进行修正。

使用光学显微镜或电子显微镜检查芯片的物理结构，该方法允许对设备，或对诸如安全装置或数据存储器等感兴趣的区域进行分析或逆向工程设计。

非破坏性攻击是智能卡在执行算法时，通过各种措施获取诸如功耗之类的定量信息来分析智能卡，这种攻击方式结合算法内部特性和算法执行时所依赖的环境特性。

1.4 加密算法原理

密码学的最基本目的：对通信或者存储的信息进行某种编码变换使得非法者无法了解通信或者存储的真正内容。

随着信息化和数字化社会的发展，人们对信息安全和保密的重要性认识不断提高。在1997年，美国国家标准局公布实施了DES，民间力量开始全面介入密码学的研究和应用中，采用的加密算法有DES、RSA、SHA等。随着对加密强度需求的不断提高，后来又出现了AES、ECC等。

1.4.1 密码体制基本概念

Alice发送给Bob的信息，通常称为明文（Plain Text），如英文单词、数字符号或数据。他首先用某个密钥（Key）对明文进行加密，得到信息称为密文（Cipher Text），然后将密文发给Bob。Bob收到密文后，能利用事先知道的密钥对密文进行解密而获得明文。密码体制几种不同的分类标准：

1）操作方式是明文变换成密文的方法。按操作方式进行分类，有替代操作、置换操作、复合操作等等。

2）按照使用密钥的数量进行分类，有对称密钥（单密钥），公开密钥（双

密钥)。

3）按照对明文的处理方法进行分类，有流密码，分组密码。

图1.2是加解密的示意图。加密系统分为对称加密系统和非对称加密系统，分别如图1.3和图1.4所示。

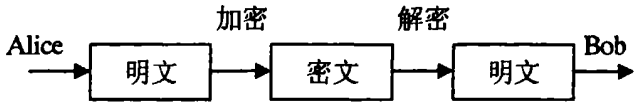

图1.2 加密/解密示意图

Figure1.2 Encrypt/decrypt illustration

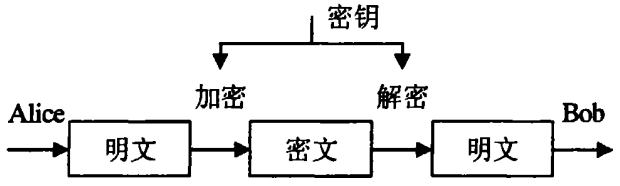

图1.3 对称密钥体制

Figure1.3 Symmetric encrypt/decrypt system

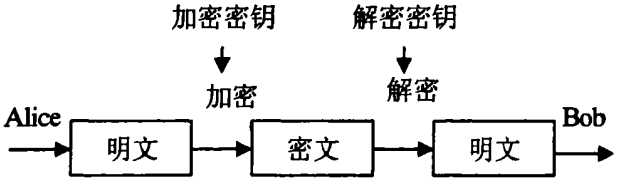

图1.4 非对称密钥体制

Figure1.4 Asymmetric encrypt/decrypt system

一个满足下面四个条件的五元组(P,C,K,E,D)为一个密码体制：

1）P是一个非空有限集合，表示所有的明文空间。

2）C是一个非空有限集合，表示所有的密文空间。

3）K是一个非空有限集合，表示所有的密钥空间。

4）对任意的$k\in K$，都存在一个加密函数：$E_k(\in E):P\to C$和相应的解密函数：$D_k(\in D):C\to P$，对任意的明文$m\in P$均有$D_k(E_k(m))=m$，其中E_k和D_k都是单射函数。

应该根据使用特点来选择加密算法，由于非对称加密算法的运行速度比对称加密算法的速度慢很多，当需要加密大量的数据时，采用对称加密算法，提

高加解密速度。对称加密算法不能实现签名，因此签名只能采用非对称算法。由于对称加密算法的密钥管理是一个复杂的过程，密钥的管理直接决定着他的安全性，因此当数据量很小时，可以采用非对称加密算法。

在实际的操作过程中，通常采用的方式是：采用非对称加密算法管理对称算法的密钥，然后用对称加密算法加密数据，结合了两类加密算法的优点，既实现了加密速度快的优点，又实现了安全方便管理密钥的优点。

一般来说，选定加密算法后，密钥越长则运行速度越慢，应该根据实际需要的安全级别来选择密钥长度。RSA建议采用1024位的数字，ECC建议采用160位，AES采用128位即可。

1.4.2 密码体制分析

通常数据的加密和解密过程是通过密码体制和密钥来控制的。密码体制必须易于使用，特别是应当可以在微型计算机上使用。密码体制的安全性依赖于密钥的安全性，现代密码学不追求加密算法的保密性，而是追求加密算法的完备。也就是使攻击者在不知道密钥的情况下，没有办法从算法找到突破口。

编码与密码体制相结合，通常的码字短语比替代的明文要短的多。这本身又提供了对明文的压缩，而且当码字是取自于任意的字符串，并不一定是有意义的实际的字、句子等时，这种编码可以具有抗通常的统计特性的密码分析。因为码字之间已不再存在字母频率等统计特征。将编码与密码体制相结合一般可产生比单独使用一种方法生成的密码体制更难以破译。原因之一是密码本包含的短语使得密码体制的密钥集合进一步扩大，另外密码本隐去了明文和密文的统计特性。

密码本存在不足，如果密码本反复使用，将给密码分析者破译密码本提供极大方便。密码本需要经常变化，由于密码本不易自动生成，所以密码本的改变以及安全传输成为密码本技术在现代密码体制应用中的主要障碍。

一个密码体制的安全性取决于破译者具备的能力。一般模型都假定 Alice 和 Bob 在一个不安全的信道上通信，而 Eve 作为第三者（或密码分析者）总是企图破译 Alice 和 Bob 之间的通信内容。

1）无条件安全（Unconditional Security）的密码体制

不论提供的密文有多少，密文中所包含的信息都不足以唯一地确定其对应

的明文；具有无限计算资源（诸如时间、空间、资金和设备等）的密码分析者也无法破译某个密码系统，则称这样的密码体制是无条件安全的，它意味着不论破译者拥有多大的资源都不可能破译。

2）计算安全（Computational Security）的密码体制

算出和估计出破译它的计算量下限，利用已有的最好的方法破译该密码系统所需要的努力超出了破译者的破译能力（诸如时间、空间、资金等资源），则称这样的密码体制是计算上安全的，计算上安全的密码表明破译的难度很大。

无条件安全的密码体制是理论上安全的；计算上安全的密码体制是实用的安全性。但目前已知的无条件安全的密码体制都是不实用的；同时还没有一个实用的密码体制被证明是无条件安全的。

针对密码体制有以下四种攻击类型：

1）唯密文攻击（Cipher Text Only Attack）——Eve 仅有一个密文串，他也知道在明文中使用的语言。

2）已知明文攻击（Known Plaintext Attack）——Eve 不仅拥有一个密文串 y，他还拥有与 y 相对应的明文串 x。

3）选择明文攻击（Chosen Plaintext Attack）——Eve 可暂时性的获得对加密部分的访问权，他能获得任意的明文串 x 及对应密文 y（这种攻击常常是通过跟踪 Alice 发给 Bob 的明文串来分析）。

4）选择密文攻击（Chosen Cipher Text Attack）——Eve 可暂时性的获得对解密部分的访问权，他能获得任意的密文串 y 及对应明文串 x。

1.4.3 好密码体制的若干特性

1）Shannon 标准

2）混淆（Diffusion）与扩散（Confusion）

3）完善保密性（Perfect Secrecy）

4）冗余度（Redundancy）与唯一解距离

5）乘积密码（Product Cipher）

6）编码与密码体制

随着计算机的发展，结合 Shannon 的 5 条标准，通常一个好的密码体制至少也应满足以下几条：

1）从截获的密文串或明文与密文串对，要确定密钥或任意明文串应在计算机上是不可行的。

2）密码体制的保密性不依赖于对加密体制的保密，而依赖于密钥的安全。

3）加密和解密算法应适用于所有密钥空间的元素。

4）密码系统易于实现和使用方便。

1.4.4 分组加密算法设计原则

有关实用密码的一般设计原则是Shannon提出的混乱原则和扩散原则：

1）混乱：所设计的密码应使得密钥和明文以及密文之间的依赖关系相当复杂，以至于这种依赖性对密码分析者来说是无法利用的。

2）扩散：所设计的密码应使得密钥的每一位数字影响密文的许多位数字以防止对密钥进行逐段破译，而且明文的每一位数字也应影响密文的许多位数字以便隐蔽明文数字统计特性。

还有其他原则包括：

1）简单性原则：包括规范的简单性和分析的简单性。

2）必须能抗击所有已知的攻击，特别是差分攻击和线性攻击。

3）可扩展性。要求能提供128、192、256比特的可变分组或密钥。

分组密码有两个重要的参数：密钥长度和分组长度。分组长度是每次操作的信息分组的大小。即对任意的明文m先分成长度为n的信息块，然后对每一个信息块使用相同的密钥k（此时密钥k的长度为n）加密，即$m = m_1 m_2 .. m_i$，其中m_i是长度为n的明文块，使用加密函数E_k得到$C = E_k(m_1)E_k(m_2)..E_k(m_i)$。

大多数分组算法的主要思想是取一个长度为n（n必须是偶数）的分组，然后把它分成长度为$n/2$的两部分：L和R。然后定义一个迭代型的分组密码算法，其第i轮的输出取决于前一轮的输出：$L_i = R_{i-1}$，$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$；$K_i$是第$i$轮使用的子密钥，$f$是任意轮函数。该函数保证了它的可逆性，异或被用来合并左半部分和轮函数的输出，它肯定满足：$L_{i-1} \oplus f(R_{i-1}, K_i) \oplus f(R_{i-1}, K_i) = L_{i-1}$。

1.5 本文的研究内容

本文对旁道攻击技术进行分类，对功耗攻击技术的特点及关键技术，特别

是差分功耗攻击（Differential Power Analysis, DPA）和高阶差分功耗攻击（High Order Differential Power Analysis, H-O DPA）技术进行研究。对新出现的针对AES的零值攻击，针对DES的重叠攻击和关联攻击等，也进行研究并提出相应的防御方法。针对DES的高阶DPA攻击，提出相应的防御方法并设计实现DES芯片。为实现这样的目的，本论文主要将要做如下几方面的研究工作：

1）研究功耗攻击的实施方法，包括SPA，DPA，高阶DPA；对功耗攻击方法进行分类；研究新出现的专用攻击方法，包括针对AES的零值攻击，针对DES的关联攻击，重叠攻击等，指出现有的一些防御方法的不足。

2）采用屏蔽方法的AES芯片不能防御零值攻击，对此提出新的防御方法。引入随机化方法和变形屏蔽方法（Transformed Masking Method, TMM）修改AES算法，同时将AES算法中$GF(2^8)$求逆运算的部分用简单动态差分逻辑（Simple Dynamic Differential Logic, SDDL）构建。并对改进后的电路进行仿真和安全性分析。

3）采用屏蔽方法的DES芯片不能防御关联攻击、重叠攻击，对此提出改进的屏蔽方法。在数据进入S盒之前不恢复密钥，而是修改S盒，使得数据在经过S盒变换后能够消除屏蔽。DES算法中同时存在异或屏蔽和加法屏蔽，引入两者之间相互安全转换的具体方法，使得算法中的敏感数据不以明文出现，能够完全屏蔽。对其安全性分析和仿真实验表明改进方法可以防御新提出的攻击。

4）针对DES加密系统，研究表明独特屏蔽方法（Unique Masking Method, UMM）及几次改进方法不能防御高阶DPA攻击，在其基础上提出算法层和逻辑层组合的防御方法，改进UMM方法；研究灵敏放大器型逻辑（Sense Amplifier Based Logic, SABL）特性，设计基于SABL的逻辑单元库，半定制设计流程，并指出用SABL逻辑实现S盒的原因。对该算法的安全性分析和仿真实验表明可以防御高阶DPA攻击。

5）分析现有DES芯片实现方法，根据DES算法的特点，设计能够防御高阶DPA攻击的DES芯片。修改原始S盒，增加1个随机数和2组S盒。采用SABL实现DES芯片关键部分模块；采用CMOS实现非关键部分模块，最后构成整体DES芯片。设计实现芯片时考虑智能卡的限制，在一些指标的选择上进行折中，采用部分流水结构。对其进行性能仿真分析并与现有芯片进行分析比较，芯片能够实现加解密，能够防御高阶DPA攻击，比以前的方法节省资源。

1.6 本文的组织结构

本文研究功耗攻击技术和相应的防御技术，对AES芯片的零值攻击，DES的高阶DPA攻击等都进行研究并提出相应的防御方法。文章的组织结构如下：

第1章是绪论，介绍课题的背景知识，课题的意义，安全IC卡的使用和工作原理，攻击智能卡的常规方法，加密算法特点等与本课题相关的一些内容。

第2章对旁道攻击方法进行分类，分析静态互补CMOS逻辑的结构和功耗特性，得到静态互补CMOS逻辑的功耗特性与数据的相关性，引入衡量抗功耗攻击的参数NED和NCD以及相应的计算方法。分析功耗攻击技术和新的功耗攻击技术的特点及关键技术，介绍了当前的一些防御方法。

第3章研究针对AES的零值攻击，指出现有防御方法的不足。提出引入随机化方法和TMM修改AES算法；介绍SDDL逻辑特性，生成SDDL单元库，将AES算法中$GF(2^8)$求逆运算的部分用SDDL逻辑构建。对改进后的电路进行仿真和安全性分析，表明可以防御零值攻击和高阶功耗攻击。

第4章研究功耗攻击DES及现有屏蔽技术，指出现有屏蔽方法是在进入S盒之前恢复子密钥，不能防御关联攻击，重叠攻击等新的攻击方法。提出改进的屏蔽方法，在数据进入S盒之前不恢复密钥，而是修改S盒，使得数据在经过S盒变换后能够消除屏蔽。提出改进的屏蔽方法DES算法中同时存在异或屏蔽和加法屏蔽，引入异或屏蔽和加法屏蔽之间相互安全转换的具体方法，使得算法中的敏感数据不以明文出现，能够完全屏蔽。对其安全性分析表明改进方法可以防御新提出的攻击。

第5章研究防御高阶DPA攻击的DES加密系统，研究表明UMM及几次改进方法不能防御高阶DPA，在其基础上提出算法层和逻辑层组合的防御方法，改进UMM算法；研究SABL逻辑特性，设计功耗平衡SABL逻辑单元库，半定制设计流程，并指出用SABL实现S盒的原因。该算法的安全性分析和仿真实验表明可以防御高阶DPA攻击。

第6章介绍目前DES硬件加密结构的特点和实现方法，根据DES算法的特点，设计能够防御高阶DPA攻击的DES芯片。修改原始S盒，增加1个随机数和2组S盒。采用SABL实现DES芯片关键部分模块；采用CMOS实现非关键部分模块，最后构成整体DES芯片。设计实现芯片时考虑智能卡的限制，在一些指标

的选择上进行折中，采用部分流水结构。对其进行性能仿真分析并与现有芯片进行分析比较，芯片能够实现加解密，能够防御高阶DPA攻击，比以前的方法节省资源。

最后是结论部分，总结全文的研究成果，并探讨了今后的研究方向。

第 2 章 旁道攻击技术

2.1 引言

旁道攻击时不需要解剖芯片，对设备要求低，攻击效果好。功耗攻击仅仅观测芯片功耗变化特征曲线，不对其进行干扰，不修改其内部数据，不会导致数据的任何改变，加密系统本身完好，非常难于监测。而且功耗特征容易观察和分析，并且不容易被掩盖或是伪造，能够暴露出芯片的实际运行状态，因此成为主要的旁道攻击手段。对这类攻击只能够通过被动防御的方法，使得攻击者观测不到信息或者观测到的信息没有用，进而保护密钥。

研究功耗攻击技术，特别是DPA、高阶DPA技术对信息安全具有重要的意义。以此为基础提出安全加密算法和硬件实现具有重要应用价值和理论价值，对功耗攻击及相应的防御方法成为一个研究热点。

2.2 旁道攻击方法分类

旁道信息泄露有很多种，在实际的旁道攻击中，主要是利用电路工作过程中的功耗、电磁辐射、运算时间等物理量与被处理数据的相关性。根据这些物理量的特点推断被处理的数据，进而获得密钥[16-22]。

旁道攻击包括功耗分析、电磁辐射分析、时序分析、差分故障分析等（在密码分析领域攻击和分析意义相同，本文也不做区分）。1997年Cryptography Research公司的Paul Kocher, Joshua Jaffe和Benjamin Jun首次提出功耗攻击的观念，进一步在1998年把其研究结果公布于公司网站上，并于1999年发表在Crypto会议上[15]。功耗攻击方法具有普遍性，能够对主流加密算法攻击，功耗攻击成本低，攻击效果好，得到广泛的研究与应用。

功耗攻击一般分为简单功耗攻击（Simple Power Analysis, SPA），DPA，高阶 DPA 等等。SPA 揭示执行操作和能耗泄露关系，而 DPA 揭示处理数据和能耗泄露关系[23]。旁道攻击方法大致可以分为如图 2.1 所示的分类。

文献[24]提出一种可发现在密码算法具体实现中可能存在的功耗攻击的分析方法,主要包括识别潜在攻击的基本理论、描述密码算法具体实现的增强

数据相关图、根据基本理论和增强数据相关图以识别不同强度功耗攻击的算法,并给出针对一种典型的AES算法防护技术的分析结果。

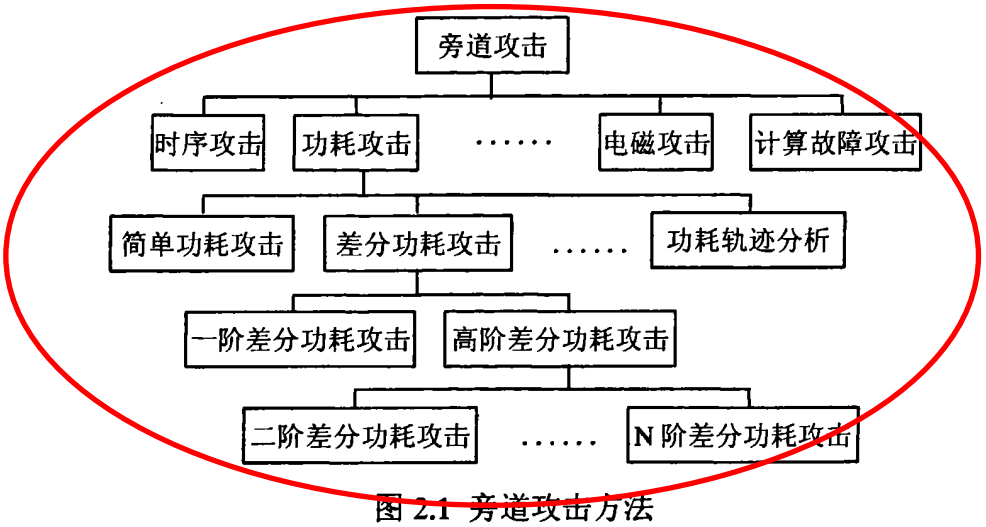

图 2.1 旁道攻击方法

Figure2.1 Side channel attack methods

文献[25]提出对于使用过防御方法的加密芯片，仍然可以用旁道攻击方法来攻击授权码消息。文献[26]提出了对ARIA[27]加密算法的功耗攻击方法。

文献[28]提出了2种新攻击方法：单比特样板攻击和通过样板增强的DPA攻击。单比特样板攻击能非常有效的区分正好在旁道样板中有很高的可能性正确的单比特；通过样板增强的DPA攻击，则是用单比特样板攻击结合传统DPA攻击。

文献[29]提出了旁道信息泄漏的仿真模型，他表明那些看上去似乎正确的近似值将导致完全错误的结构。文献[30]提出了从CMOS电路的逻辑信息直接评估DPA泄漏，该模型是基于每个门的跳变概率，自然应用到各种真实的设备来仿真能耗分析。

2.3 电磁辐射、时序攻击和故障攻击

Huiyun Li 等介绍了电磁辐射攻击[31]，提出了一个在保密处理器的设计阶段时，系统规划仿真方法来确定和估算电磁辐射泄漏特点。电磁辐射具有方向性，激发电磁场变化的电流也不仅限于电源电流，而且利用一个解调探测器可以同时探测多个电磁信号，因此电磁辐射比功耗包含更多的信息，但是电磁辐射分析方法较为复杂[32-34]。电磁仿真方法包括电流仿真，芯片版图寄

生提取，然后在处理数据时来仿真电磁辐射或者调制的辐射。同步和异步处理器表明，同步处理器的数据与 EM 辐射有关，异步处理器的数据与时间有关，这个时间在差分 EM 分析中能被观察到[31]。

密码系统进行加密运算所需要的时间不仅仅与加密算法有关，而且与输入数据有关。如 RSA 加密芯片的执行时间和他们的密钥值就存在极大的相关性。RSA 算法的基本操作是模幂运算，在平方-乘积的算法中，可以看出每一次迭代，由于幂指数不同导致算法中间的状态表达式不同的路径。幂指数是 0，仅仅执行一次模平方运算；幂指数是 1，则执行一次模平方和一次乘法运算。因此幂指数不同导致计算时间不同，整体算法运算时间与密指数有关联。如果攻击者可以观测比较采用平方-乘积算法的几次迭代执行时间，就可以推断出相关的密指数。对时序攻击进行改进，只要算法运行总时间变化，都可以进行攻击。

时间攻击[35]要求对执行时间进行精确测量而且易于防范，所以相关研究报导较少[16]。防御时序攻击的主要方法是保证算法执行时间恒定，但是这个理想状态很难达到。在实际使用中一般采用随机打乱时序，随机延迟，增加噪声等防御方法。增加采样样本，并且借助先进的数字处理技术，这些方法的防御作用就可以被消除。

在加密运算中，硬件故障或软件错误会导致数据错误，如果能够控制这种错误，使错误数据按照攻击者要求运行，则可以获得一些信息。文献[36]提出的差分故障分析（Differential Fault Analysis, DFA）是一类特殊的旁道攻击，文献[37, 38]随后对其进行了改进，攻击者通过制造电源或时钟信号的“毛刺”、破坏电路等方法注入故障，然后分析故障电路的工作结果获得密钥。故障攻击需要控制错误计算，攻击的难度、强度和方法随攻击者对于故障发生的位置、时刻的控制能力不同而异[39]，一般来说攻击实施难度较大。而且通过入侵检测和信息校验可以发现故障，进而启动保护措施，比如锁定芯片运行，向高层报警等阻止攻击。文献[40]通过添加保护电路来防御 DFA，通过该电路，所有诱导 DES 芯片寄存器的单向错误都可以被检测出来，并且立即向加密系统报警。

由于功耗攻击是最主要的芯片实现攻击手段，而且功耗和电磁辐射都是与电路的工作电流有关的物理量，所以更多的文献重点研究功耗攻击以及对

应的防御方法。功耗分析还可以和电磁辐射分析、时间攻击、故障攻击等方法组合使用，组合攻击往往比单一途径的分析方法更加有效[16, 39, 41, 43]。

2.4 功耗攻击的物理基础和衡量防御能力的参数

现代加密设备大多数使用半导体逻辑门构建，而其中静态互补CMOS逻辑是使用最广泛的一种逻辑类型。当加密设备处理数据时会消耗能量，而且功耗特征与处理的数据有关联。功耗攻击的物理基础是集成电路某个时刻的功耗与该时刻前后的电路状态相关，其中的电路状态是指电路内部所有状态保持节点以及输入信号的状态组合。此外，集成电路功耗中还包括噪声功耗和由于外界环境噪声引起的功耗噪声，这些功耗与数据无关。

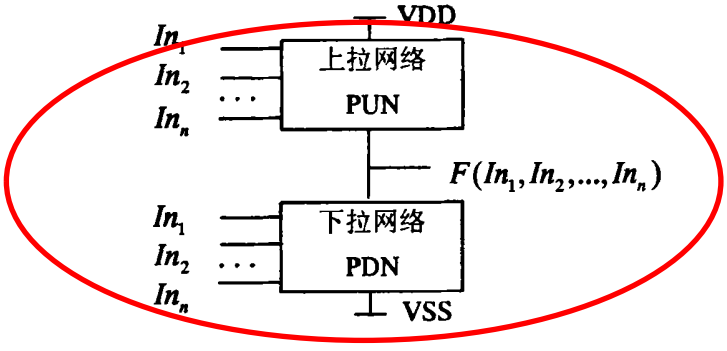

图2.2 静态互补CMOS逻辑结构图

Figure2.2 Static complementation CMOS logical structure

静态互补CMOS逻辑门由上拉网络（Pull-Up Network, PUN）和下拉网络（Pull-Down Network, PDN）组成，其结构如图2.2所示。图中显示了一个通用的具有N个输入的逻辑门，它的所有输入都同时分配到上拉网络和下拉网络。PUN的作用是每当逻辑门的输出意味着逻辑1时，它将提供一条在输出结点和电源VDD之间的通路。同样，PDN的作用是当逻辑门的输出意味着逻辑0时将输出结点连接至地VSS。逻辑门的PUN和PDN网络是互补的，因此当逻辑门处于稳态时两个网络有且只有一个导通。一旦瞬态过程完成，总有一条导通路径存在于VDD和输出端F或VSS和输出端F之间。

CMOS逻辑门的功耗由动态功耗与静态功耗两部分组成。动态功耗只发生在逻辑门开关的瞬间，它由直流通路电流功耗与电容充电功耗两部分组成。在没有开关活动存在时，电源和地之间仍然存在一个很小的电流，即漏电流，

静态功耗是指由漏电流引起的功耗。

逻辑门的输入信号的变化时间不可能为0，相应的输出信号的变化时间也不可能为0，也就是说输入输出信号的跳变需要一定的时间。这就造成了逻辑门在开关过程中VDD和VSS之间短期内出现一条直流通路，此时上拉网络与下拉网络同时导通。直流通路功耗很大程度上决定于输入信号的上升下降变化时间。当逻辑门的输入信号发生变化引起输出信号由低电平跳变为高电平时，电源要对电容充电。电容充电功耗比直流通路功耗要大得多，它占了整个动态功耗的大部分。动态功耗与逻辑门的开关频率有关，开关频率越高，动态功耗越大。静态功耗是在没有开关活动存在时电源与地之间的电流与电源电压的乘积。一个CMOS门的功耗由许多因素决定，其中包括输出端的翻转、负载电容、自身电容、时钟频率、供电电压以及翻转电压[44]。

电路的功耗模型可以表示为[45]：

$$P_{total} = P_{switch} + P_{short\_circuit} + P_{leakage} \tag{2-1}$$

（2-1）式中 P_{switch} 为逻辑门翻转引起负载电容充放电形成的功耗，占功耗的大部分，$P_{short\_circuit}$ 为短路电流功耗，$P_{leakage}$ 为泄露电流功耗。随着工艺的发展，集成度的提高，$P_{leakage}$ 在 P_{total} 中占的比例在增加，P_{switch} 占的比例在缩小。但 P_{switch} 与逻辑门是否翻转有关，也就表明电路中运行的数据的 0，1 状态与功耗信号必然有一定的相关性。

只有输出信号发生 0→1 跳变时，电源才对电容进行充电；而在其它三种情况（0→0、1→1、1→0）下，电源并不对电容进行充电，因此可以很容易地将前者与后者区分开来。微观来看电路中的逻辑门翻转消耗能量可以知道这种相关性，当输出信号发生 0→1 跳变时，反相器的功耗明显大于发生其它三种跳变时的功耗。因此功耗与密码模块中运算的数据具有一定的相关性，即加密电路的功率信号与密码系统的密钥及敏感数据存在相关性，功耗分析的原理正是基于这种相关性。

为了衡量电路防御功耗攻击的能力，文献[46]提出了功耗变化幅度的计算公式（2-2）。以每个周期来计算功耗，标准功耗偏差（Normalized Energy Deviation, NED）是最大和最小功耗之间的差与最大功耗的比值：

$$NED = \frac{Max(energy/cycle) - Min(energy/cycle)}{Max(energy/cycle)} \tag{2-2}$$

同样的，标准电流偏差（Normalized Current Deviation, NCD）是最大和最小电流之间的差与最大电流的比值。因为有些电路是包含预充电阶段的，一个时钟周期有预充电和求值两个阶段，对应两个不同的电流峰值，需要分开定义 NCD，可以计为 NCD_p 和 NCD_e，即式（2-3）和（2-4）。

$$NCD_p = \frac{Max(Current_p) - Min(Current_p)}{Max(Cuurrent_p)} \tag{2-3}$$

$$NCD_e = \frac{Max(Current_e) - Min(Current_e)}{Max(Cuurrent_e)} \tag{2-4}$$

NED和NCD是[0，1]间的一个值，都是是衡量电路功耗变化大小的参数，他们确定功耗与处理数据的相关程度，该值越大，表明功耗变化越大，功耗泄漏的旁道信息越多，就越容易受到功耗攻击。反之亦如此。文献[47]认为，不需要功耗差分为0，只要其没有规律，不反映运行时的信息即可。就是说只要功耗差分为随机数，不一定要为0。

2.5 功耗攻击技术

2.5.1 功耗攻击芯片实施方法

一个轨迹样本可以得到一组测量的能量值，例如，一毫秒算法执行操作，在 5MHz 的采样频率下能够包含 5000 个点。装备良好的电子实验室中都备有能够对电压变化进行数字化抽样的设备，而且抽样频率可以超过 1GHz，精确误差小于 1%[15]。

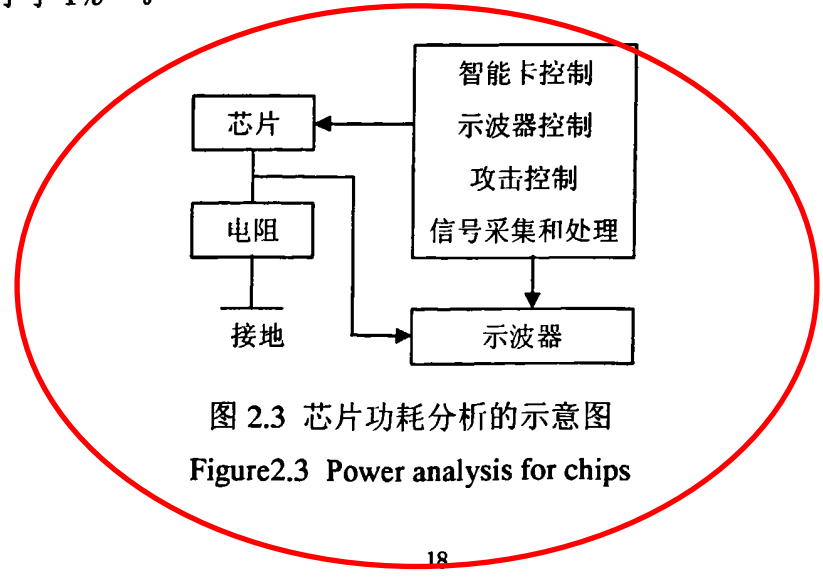

图 2.3 芯片功耗分析的示意图

Figure2.3 Power analysis for chips

如图 2.3 所示，在芯片电源输入端或接地端插入一个串联的小电阻（如 50 欧姆）。当芯片运行时有电流经过该电阻，所获得的电流变化信息可以用来分析得到芯片的密钥，具体攻击流程如图 2.4 所示。

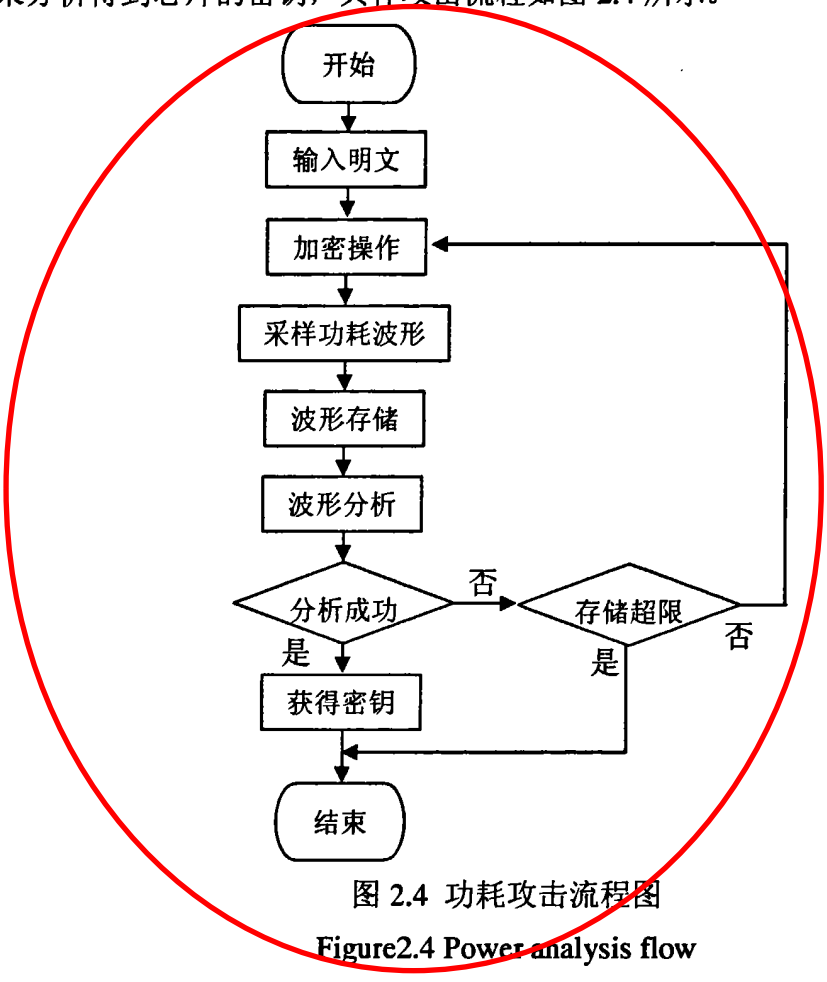

图 2.4 功耗攻击流程图

Figure2.4 Power analysis flow

密码模块的功耗信息不仅仅依赖于密钥，还和其它许多信息有关，可以用各种方法增强与密钥的相关性，而压制其它信息的干扰。

攻击者建立一个攻击模型分析得到的波形信息，一般来说，只需要一些很简单的模型就可以得到密钥值。如图 2.5 所示，旁道攻击先假设芯片运行时泄露模型信息特征，用猜测的密钥进行理论计算，得出模型期望的信息特征；然后输入数据实际运行芯片，观察记录芯片实际泄露的特征，将两者进行相似度比较，进而得出两者的相关系数。根据相关系数来判断猜测得密钥是否正确，以期得到正确的密钥。

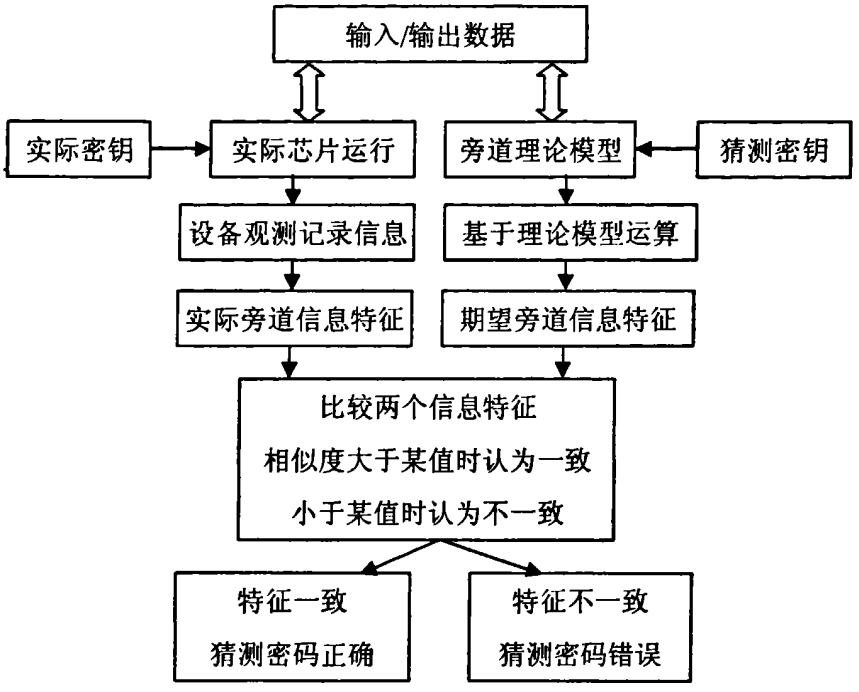

图 2.5 旁道攻击的原理

Figure2.5 The principle of side channel attack

2.5.2 SPA 攻击方法

SPA攻击方法中，芯片功耗大小随微处理器执行的指令不同而不同，攻击者直接观察测定芯片运算时的功耗，找到特定逻辑门带来的功耗影响，从而判断芯片内部的工作情况，进而破解加密系统。攻击者通过观测功耗能够得到关于设备的运行信息以及密钥信息，只是能耗信息通常非常小；能够知道所处理数据的海明权重或者知道执行的是什么分支结构。芯片中一些大的工作特点，如DES的每一轮操作以及RSA的模乘-平方等操作变化很明显。智能卡处理这些操作时会在一些时段出现较大的区别，这些都可以通过直接观察功耗波形来进行区别。SPA方法简单，但因为是直接观察系统的功耗，需要对电路的工作原理有很深的了解。

在高精度的测量下，智能卡中执行的指令的差异可以被观测出来，例如RSA算法中乘法运算与平方运算之间的差异；DES算法中置换和移位操作之间的差异。SPA通过这些区别来攻击加密算法，被证实有一定的可行性[15]。

SPA通过平均的措施将外部噪声消除，但没有消除算法噪声，只能用于

分析智能卡等结构简单的电路。如果算法实现中存在数据依赖分支，即分支条件与数据有关，则SPA将非常有效。如RSA存在分支条件，SPA对其攻击就非常有效。

有很多方法来对抗SPA攻击，一般可以将指令顺序随机打乱或是程序流程打乱来混淆功耗。执行随机空代码或者避免内存读取在寄存器中运行的数据，也可以防御SPA攻击。

加密芯片产生的功耗信息幅值非常小，信号之间的串扰，衬底耦合噪声，地弹噪声等都可能会淹没功耗信息。因此在功耗攻击时，需要了解电路的噪声情况，这些噪声主要包括两部分：1）密码模块电路本身的噪声，如热噪声，容性耦合噪声等；2）算法级噪声，主要是整个电路中与密码运算无关的其他逻辑门的功耗噪声。由于测量目标是整个芯片中的一部分逻辑门，相对来说，其他逻辑门的功耗都是一种噪声。对前一类噪声，可以小心使用测量装置，好的电路设计经验和滤波等方法来降低。对后一类噪声，则可以使用求平均值来消除其影响。

为了防止攻击者分析功耗信息，设计者会插入伪随机噪声或白噪声来淹没真正的功耗信息，但是利用数字信号处理技术和自适应滤波可以消除外加的噪声信号。

文献[48]给出用SPA攻击Camellia[49]算法密钥表的方法，该攻击方法适合智能卡在运行时泄漏数据海明权重的情况，用海明权重来推测所有的密钥位。他证实通过精确的功耗分析数据可以非常快得到密钥，并且不需要任何明文和密文。

2.5.3 DPA 攻击的前提条件

DPA攻击的前提条件是在算法执行中，存在一个或多个中间变量，能够由很少的密钥比特位数和输入（输出）数据决定。也就是说存在中间变量依赖于很少的一部分密钥（一般少于32位）。如果能够记录芯片运算时功耗变化的情况，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，进而破解全部密钥。在实施攻击过程中，攻击对象是依赖少于32比特密钥的数据；依赖高于32比特的数据，对其实施攻击代价太大，失去了旁道攻击的意义。

以 DES 加密算法为例来说明这个前提条件，DES 中 S 盒运算是唯一的非线性运行部分，如图 2.6 所示，S 盒输出的某一位仅取决于其输入的 6 位：

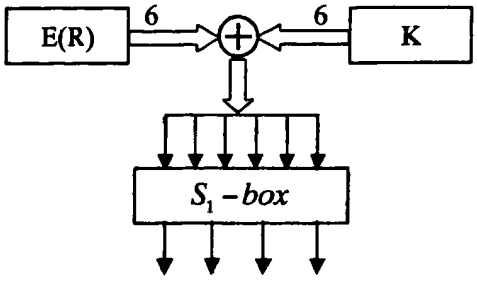

图 2.6 S 盒输入输出

Figure2.6 Input/output of S-box

S盒的输出变量是中间变量，并且依赖于很少的密钥，这里仅仅依赖于密钥中的6位，满足DPA攻击的前提条件。

2.5.4 差分功耗攻击

Paul Kocher 等人[15]提出实际的旁道攻击，特别是 DPA，其优异的攻击特性引起人们的重视。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攻击方法，不需要知道被攻击芯片的具体内容。该技术利用加密运算的特点和统计分析技术来推测加密系统中的关键信息，即利用它们获取保存在智能卡内部的数据，而且搜索的密钥空间大大小于目前已知的几种密码分析方法，只需要大约 1000 次加密，几乎可以破解所有的智能卡。他们的研究表明，没有任何防御措施的智能卡将容易受到攻击。

DPA利用不同数据对应的条件功耗分布的差异推断数据，它是一种统计分析方法，统计分析方法的抗噪声能力强于SPA，而且更加难以预防，应用更为广泛。SPA攻击主要利用可见的重复采样和对芯片技术的了解来识别相关的功耗波动，而DPA攻击则使用统计分析和误差修正技术来提取与密钥相关的信息，那些SPA可能感觉不到的信息通常可以用DPA方法提取出来。一个完全不懂得智能卡技术的编程人员完全可以利用专用程序对没有DPA防范的智能卡芯片实现攻击。除了指令的执行顺序会影响功耗外，指令执行时所处理的数据也会影响功耗，这种影响虽小，有时更会被噪声或错误的量测所覆盖消耗，但依靠统计的方式还是可以看出端倪。DPA是一种以功耗曲线图

为基础，再以统计方式推演主密钥的攻击技术。它分为数据收集阶段、数据分类阶段与数据分析阶段。

DPA一般满足以下几条规则：

1）密码模块使用固定密钥加（解）密，攻击者可以用它来加（解）密随机输入的数据，同时测量密码模块的功耗。

2）攻击者能够知道功耗曲线对应的加（解）密运算的明文（密文）。

3）加（解）密运算的中间结果仅仅依赖于明文（密文）和少量的密钥位。

4）加（解）密运算的功耗与处理数据有相关性。

DPA具体方法如下[39, 50, 51]：

假设密码芯片运算时内部存在一个中间结果满足：它的取值可由部分密钥和密文（或者明文）确定；它的值不同则对应芯片功耗不同。则可以用下述方法推断与这个中间结果相关的部分密钥，定义该中间结果为划分函数D。

假设D=b，b是一个单位的中间结果，它是密文和密钥的函数，电路使用相同的密钥对N组不同的明文加密，得到N组密文，同时记录下相应的功耗曲线样本$P_0,P_1,\cdots,P_{N-1}$；采样的时间间隔为Δt，每条测得的样本曲线由m个采样点组成，记为$P_i=[P_i(0),P_i(1),\cdots,P_i(m-1)]$，$P_i(j)$对应$t=j\Delta t$时刻的功耗值，其中$i=0,1,\cdots,N-1$，$j=0,1,\cdots,m-1$，$m$定义为$P_i$的长度。

假设密钥为k_j，则可计算出功耗样本曲线对应的划分函数$D_0,D_1,\cdots,D_{N-1}$，按照划分函数的取值将样本分为2组，分别用$X_0,X_1,\cdots,X_{N1}$和$Y_0,Y_1,\cdots,Y_{N2}$表示。

定义 2.1 N条长度为m的样本曲线$P_0,P_1,\cdots,P_{N-1}$，曲线$\overline{P}=[\frac{1}{N}\sum_{i=0}^{N-1}P_i(0),\frac{1}{N}\sum_{i=0}^{N-1}P_i(1),\cdots,\frac{1}{N}\sum_{i=0}^{N-1}P_i(m)]$称为$P_0,P_1,\cdots,P_{N-1}$的均值曲线。

设$\overline{X}$和$\overline{Y}$分别是两组样本曲线的均值曲线。

定义 2.2 定义两个长度为m的曲线$\overline{X}$和$\overline{Y}$的差分曲线为$\overline{X}-\overline{Y}=[\overline{X}(0)-\overline{Y}(0),\overline{X}(1)-\overline{Y}(1),\cdots,\overline{X}(m-1)-\overline{Y}(m-1)]$。将差分曲线的各采样点取绝对值后得到的曲线称为他们的绝对差分曲线，即$|\overline{X}-\overline{Y}|$。

如果在绝对差分曲线中存在明显的峰值，则认为假设的密钥正确，否则假设的密钥错误。用类似的方法可以依次推测出密钥的其他位。

两组样本曲线的绝对差分曲线的最大值称为样本差分，样本差分对应的

相关点称为敏感相关点。Messerges证实，如果敏感相关点能够用某种方法找到，软件在智能卡上的应用将被攻击[50]。找到DPA的敏感相关点，已经成为一个研究难点和热点。

文献[51]提出一种通过改进随机模式来优化差分旁道密钥分析芯片系统的方法。他在一个合适的向量子空间近似于真实的泄漏函数，在合适的情况下仅仅要求一个测试的密钥。

文献[52]用0.18 μm CMOS实现了基于AES的嵌入式加密处理器，分别用波分动态差分逻辑（Wave Dynamic Differential Logic, WDDL）和普通标准逻辑单元实现它，进行了防御DPA攻击的性能分析比较。对普通逻辑单元的攻击仅仅需要8000次样本，而同样的用WDDL逻辑的在获得1500000次样本时仍然不能揭示密钥。这个改进至少提高了2个数量级，使攻击变得不可行。

2.5.5 高阶 DPA 攻击及改进方法

高阶DPA中最常见的是二阶DPA，Messerges第一次报道了用二阶DPA成功攻击芯片的例子[53]。文献[54]系统的描述二阶DPA攻击智能卡，给出的方法对智能卡的攻击是可行的。攻击所需的准备很简单，很容易估算复杂度，并且能够攻击任何已经采用添加屏蔽方法防御DPA的芯片。攻击一个应用在8位微控制器上的已经屏蔽过的AES，需要不超过400个轨迹样本。

用一个简单例子说明二阶 DPA 攻击思想，用伪代码写的算法 W1 和 W2 的部分片段，算法开始是组合输入 PTI 数据和密钥。组合这一个步骤有时也称为“白化处理”，数据白化处理这个常规方法在很多算法中是第一步执行的。白化处理数据是通过异或操作执行的，白化处理被证实是一阶 DPA 攻击的受害者。对白化处理方法进行改进来防御一阶 DPA 攻击，然而随后证实改进后的方法是二阶 DPA 攻击的受害者。

W1 算法在 A 行执行异或操作，不幸的是在 A 行执行异或操作泄露了密钥的信息。因此 W1 算法是一阶 DPA 攻击的可能受害者。

W2 算法不是直接将密钥异或 PTI，而是先产生随机数对 PTI 进行屏蔽，然后才将屏蔽后的 PTI 异或密钥。因此在 C 点的能耗与密钥以及 PTI 都没有关联，可以防御一阶 DPA 攻击，但是不能防御二阶 DPA 攻击。

二阶 DPA 攻击的基本思路是同时收集 B 点和 C 点的能耗，得到这 2 点

之间能耗差的绝对值。采集 N 个输入样本，得到这些绝对值的平均值，据此来判断密钥的值[53]。

```
Algorithm W1(PTI)
{
A:Result=PTI⊕SecretKey
…
other operations…
…
return CTO
}
Algorithm W2(PTI)
{
B:RandomMask=rand()
  mPTI=PTI⊕RandomMask
C:Result=mPTI⊕SecretKey
…
other operations…
…
return CTO
}
```

算法 W1 中 A 运算步骤是一阶 DPA 攻击的受害者，算法 W2 中 B，C 运算步骤是二阶 DPA 攻击的受害者

Messerges 假设在实施 DPA 攻击时，首先产生随机屏蔽值，并且和数据进行异或，然后再将异或后的数据和密钥进行异或操作。DPA 攻击目标是密钥字节和已经屏蔽过的数据的异或操作。如算法 W2 中的 B 至 C 的 3 行代码所示。看典型的屏蔽密钥的例子的代码，来分析 Messerger 攻击的方法。

```
t=1：m=rand()        /*产生屏蔽字节*/
t=2：x=p⊕m           /*将明文进行异或屏蔽*/
t=3：y=x⊕k           /*用屏蔽过的明文异或密钥*/
```

能耗轨迹中 $S_j[t=1]$ 是对应屏蔽产生时刻的点，$S_j[t=3]$ 是对应屏蔽数据

异或密钥时刻的点，在攻击时 2 个点相减。这 2 个能耗样本的联合分布使得可以一个一个比特获得密钥。对明文中的每一个比特，攻击者计算平均值：

明文的比特是 0 时：$\overline{S_0} = \sum_j |S_j[t=1] - S_j[t=3]|$

明文的比特是 1 时：$\overline{S_1} = \sum_j |S_j[t=1] - S_j[t=3]|$

如果 $\overline{S_0} - \overline{S_1} > 0$，那么密钥的比特是 1，否则密钥的比特是 0。

在这个攻击中，必须用差分的绝对值，否则任何情况下差分的平均值就是 0。而且必须是能耗轨迹大致相同的平均值，否则也不能得到结果。大致相同这个特征能够用统计学上的平均数距离（distance-of-mean）测试或者泊松相关系数来获得。

DPA攻击DES步骤如下[55]：

步骤1：猜测K16中的6比特密钥；

步骤2：初始化A1=A0=0；

步骤3：执行一次DES加密算法，得到一个加密输出C和相应的功耗曲线；

步骤4：计算D函数，该函数与密文和猜测的密钥相关；

步骤5：如果D=1，相应的功耗曲线放到A1组中；

步骤6：如果D=0，相应的功耗曲线放到A0组中；

步骤7：如果所得功耗曲线不足以进行似然估计，就转回到步骤3；

步骤8：分别计算A0和A1组中的平均功耗曲线，得E（A0）和E（A1）；

步骤9：计算DPA的偏差，如果偏差为0，则猜测密钥错误；如果偏差不为0，则猜测密钥正确；

步骤10：以此方法继续推测K16的其它密钥，直至获得48比特密钥；

步骤11：以所获得的K16推导R16和L16，进行K15密钥的猜测，直至全部子密钥破译。

步骤4中D函数如下：$D = C1 \oplus S1\_box(C6 \oplus K16)$

当D是表示第一位输出时，C1为密文CL的第1位比特，C6为密文E（R）的6位比特，K16为第十六轮的子密钥K进入第一个S盒的6位比特，如图2.7所示。根据最大似然估计定理可知，上述DPA攻击方法的实质意义是如果功耗偏差近似为0，就认为步骤1中猜测的6比特密钥不正确；如果功耗偏差比较明显，则可以认为猜测正确。

进行 DPA 攻击。选择 N 组明文输入，用同一个密钥运行 N 次，记任意

一次运行为PT_i，对PT_i采样并记录其消耗功率$S_i[j]$。选择分割函数$D(*)$，根据D值，将采样记录$S_i[j]$分成两部分S_0和S_1。再分别计算两部分的平均值$A_0[j]$和$A_1[j]$，得到 DPA 偏移量数组为$T[j]=A_0[j]-A_1[j]$。根据偏移量大小可以猜出密钥的一个子集，进而得出密钥。DPA 攻击方法中分割函数$D(*)$的选择，$D=C_l \oplus f(C_r,K_{16})$，将式中各个变量具体化，可得到 8 个不同的$D$函数，$f$是 DES 加密运算中的一个$S$盒函数。$K_{16}$是第 16 轮 6 比特子密钥中的子集。

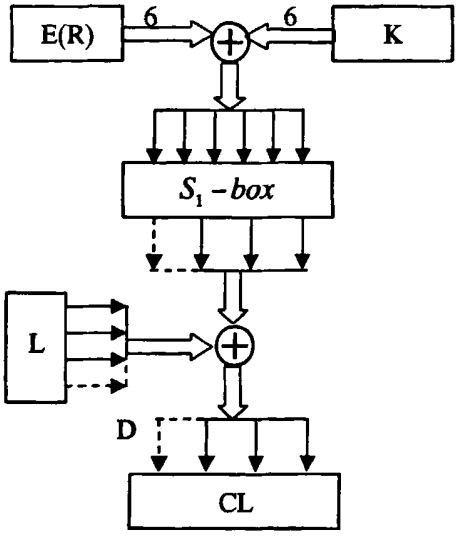

图 2.7 分割函数 D

Figure2.7 Division function D

文献[56]对Messerges提出的二阶DPA进行了精确分析，填补了其空白。指出当前研究二阶DPA攻击的一些文献其结论是正确的，但是分析过程却是错误的。并且考虑更普通的情况，介绍在普通海明距离模型的一个扩展的分析方法。

Oswald等人对二阶DPA攻击方法改进，提出基于海明权重的简单功耗泄露模型[54]，该方法是通用的并且容易实现和分析。他首先假设处理器的实时能耗依赖于所处理数据的海明权重，处理器泄露所处理数据的海明权重的信息，再假设处理数据时消耗的能量与海明权重是大致的线性关系，即海明权重大的消耗能量多，海明权重小的消耗能量小。研究证实这些假设是合理的，当今很多智能卡处理器精确的呈现了这个特点。

用 P[j]表示在特定时刻 j 的能量消耗。P[j]能够分成 3 部分。第一部分是正在处理的数据的海明权重的变量，第二部分是固定的附加部分，第三部分是噪声。这个简单的线性关系可以表示为：

$$P[j]=\varepsilon\cdot d[j]+L+n \tag{2-5}$$

式（2-5）中 $d[j]$ 表示在时刻 j 中间变量数据的海明权重，ε 表示对海明权重每增加一个“1”能耗增加的数量，L 表示总的附加的固定能耗部分，n 表示噪声。噪声 n 的平均值假设为 0，因此当用大量样本统计时，噪声能被忽略。

假设 $a\in\{0,1\}^n$，$C(a)$ 表示 a 的能耗。当正在处理 a 时，设备能耗 C 与 a 的权重成正比，即 $C(a)\sim HW(a)$。

假设 $a,b\in\{0,1\}$，$HW(x)$ 表示 x 的海明权重，则：

$$HW(a\oplus b)=|HW(a)-HW(b)| \tag{2-6}$$

从式（2-6）知道能够根据 $HW(a\oplus b)$ 来预测 $|C(a)-C(b)|$。

Messerger 的原始方法是预测中间结果单独的比特，而 Oswald 的方法是预测几个比特，因此 Oswald 方法更通用。

DPA 是难以防御的，由 P.Kocher，J.Jaffe 和 B.Jun 提出的，然后由 T.Messerges 正式化的高阶 DPA 攻击能力更强，更加难以防御。高阶 DPA 研究秘密数据和功耗曲线中几个点的关联（而不是 DPA 攻击中的一个点），该方法最困难的是确定所关注的操作数据运行的准确时刻，这导致高阶 DPA 攻击难度增加，限制了高阶 DPA 攻击的使用。基于该功耗分析技术，很多文献给出了各种改进方法，使得高阶 DPA 变得更简单。对以前提出的对抗 DPA 的各种方法也给出了新的攻击方法，如重叠攻击，改进型二阶 DPA 攻击等。

高阶攻击适用在这样一种情况。存在某个中间值（或值的集合），它仅仅依赖于明文和密钥的一小部分，但是在任何特定时刻，他都不直接和能耗关联。相反，这个值关联计算时的一些时刻能耗的联合分布。

高阶DPA攻击方法与一阶DPA类似，区别的关键在划分函数。D=1^n时，相应的功耗曲线放入A1；D=0^n时，相应的功耗曲线放到A0中；而D不等于1^n或者0^n，则丢弃该曲线不用。就是说n阶（即高阶）功耗分析是指从输出的1个字节中选择n位，关联几个值来得到重要数据的能耗，分析这n位功耗与整个功耗曲线的统计关系，攻击需要的样本数据量和计算量远远大于一阶DPA。

高阶DPA（n阶DPA）过程如下：

步骤1：猜测K16中的6比特密钥；

步骤2：初始化A1=A0=0；

步骤3：执行一次DES加密算法，得到一个加密输出C和相应的功耗曲线；

步骤4：计算分割函数D，该函数与密文和猜测的密钥相关；

步骤5：如果$D=1^n$，相应的功耗曲线放到A1组中；如果$D=0^n$，相应的功耗曲线放到A0组中；

步骤6：如果$D\neq 1^n$，或者$D\neq 0^n$，则相应的功耗曲线弃之不用；其中n是D函数的位数，是功耗攻击的阶数，例如2阶，则n=2，则$1^n=11$，$0^n=00$

步骤7：如果所得功耗曲线不足以进行似然估计，就转回到步骤3；

步骤8：分别计算A0和A1组中的平均功耗曲线，得E（A0）和E（A1）；

步骤9：计算DPA的偏差，如果偏差为0，则猜测密钥错误；如果偏差不为0，则猜测密钥正确；

步骤10：以此方法继续推测K16的其它密钥，直至获得48比特密钥；

步骤11：以所获得的K16推导R16和L16，进行K15密钥的猜测，直至全部子密钥破译。

DPA 的阶数越高，攻击能力越强，功耗偏差越明显，则猜测密钥正确的概率也越大，但是高阶 DPA 需要的数据量和计算量很大，应根据所遇到的具体情况来决定选择一阶还是高阶 DPA。

高阶 DPA 攻击方法中如何确定敏感相关点的时刻。Waddle[57]等人发现相对于标准 DPA 攻击，能通过方法减小高阶攻击额外的工作，提出在能耗轨迹上增加合适的点来产生 DPA 峰值。他们提出了两种方法来找到敏感相关点：零值补偿（Zero-Offset） 2DPA 和快速傅立叶变换 2DPA，他们都是二阶 DPA 的变体。

1）零值补偿 2DPA

零值补偿 2DPA 应用在特殊的情况下，当 2 比特的能耗关联时刻是同时发生时（例如，随机比特 r 和屏蔽后的比特 r+b 的能耗关联是同时的）。如果屏蔽值和屏蔽是同时处理，则零值补偿 2DPA 能够凑效，这样的话只需要关注一个点。同时处理的一个例子是在设计成对电路时，屏蔽值和屏蔽并行处理。零值补偿 2DPA 的一个变形是已知补偿 2DPA，当屏蔽值和屏蔽不是同时

处理，但是一个已知数，则可以用类似的方法。

2）快速傅立叶变换 2DPA

快速傅立叶变换（Fast Fourier Transform, FFT）2DPA 应用到更一般的情况下，攻击者不知道关联时刻，他通过很少的预计算来找到关联，但是这需要更多的功耗样本数。FFT 2DPA 本质上是一个能耗轨迹快速傅立叶变换的 DPA。FFT 2DPA 比零值补偿 2DPA 更通用，它不需要知道同时处理的关联时间，也不需要知道随机比特 r 和屏蔽后的比特 r+b 处理的时间。他用傅利叶变换来计算轨迹和自己的关联——采用自相关（autocorrelation）技术。

Jason Waddle 研究这两种方法后的结论是由于预处理步骤，所需要的样本数比原来方法要显著增加。Peeters 等人应用一个与零值补偿 2DPA 类似的方法攻击一个 FPGA[58]。他们得出的结论是零值补偿 2DPA 想法能够凑效，但是所需的轨迹样本数比标准 DPA 明显要多。这个结论与 Waddle 结论是一致的。

Jason Waddle 已经分析了 DPA 峰值的高度与样本数量和在确定信噪比的能耗模型之间是如何相关的。他给出了理论基础并且允许在理论上对特定模型估算高阶攻击的效果[57]。

2.6 新的功耗攻击技术

很多研究人员根据具体加密算法的特点，提出了各种改进的功耗攻击方法，攻击能力更强，或者能够攻击某些已经采用一定防御方法的加密算法。

2.6.1 关联功耗和重叠攻击

关联功耗分析[59]是DPA的一个改进。他假设目标S盒输出的海明权重，并且对假设的统计进行评估。能耗轨迹 $P_n(t)$ 和假设 H 之间的相关系数 $\rho_{(P(t),H)}$ 计算如下：

$$\rho_{(P(t),H)} = \frac{\mathrm{cov}(P(t),H)}{\sqrt{\sigma^2_{P(t)} \cdot \sigma^2_H}} \tag{2-7}$$

式（2-7）中 $\sigma^2_{P(t)}$ 和 σ^2_H 分别是 $P_n(t)$ 和 H 的平方差，$\mathrm{cov}(P(t),H)$ 是这2者的协方差。相关系数 $\rho_{(P(t),H)}$ 是归一化值，即 $-1 \le \rho \le 1$。$\rho = 1$（$\rho = -1$）表示 $P(t)$ 和 H 变量是完全同向相关（完全反向相关），$\rho = 0$ 表示根本没有关联。攻击

者计算每一个假设密钥的关联值，然后选择关联表现最强烈的密钥。通常CPA比DPA攻击效果更好，因为他的假设是基于几个比特，而不像DPA攻击那样基于一个比特。

文献[60]介绍了一种新的二阶 DPA 攻击方法，即重叠攻击，理论上它是二阶 DPA 攻击，在实际操作过程中和一阶 DPA 攻击一样简单，并且非常有效。他的基本思想是，二阶 DPA 攻击中最困难的是确定所需操作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，据此给出了攻击方法。依据这个思路，攻击者可以得到 S 盒的输出：

$$\begin{aligned} T &= (S'(E(R_{15})\oplus K_{16})\oplus R')\oplus(S'(E(R_1)\oplus K_1)\oplus R') \\ &= S'(E(R_{15})\oplus K_{16})\oplus S'(E(R_1)\oplus K_1) \end{aligned} \tag{2-8}$$

式（2-8）中 R' 是扩展排列后的屏蔽右边部分。可以看出 T 值不依赖于随机屏蔽值，并且 R_1 和 R_{15} 一般是已知的。考虑到这一点，很容易看出通过猜测第一轮和最后一轮的子密钥的 26 位比特，来猜测第一轮和最后一轮的 S 盒输出值的异或是可能的。然后可以执行标准 DPA 攻击来找出 K_1 和 K16 的子密钥。

重叠攻击算法如下：

步骤 1：关联第一轮和最后一轮（通常是将功耗曲线进行加或减）。

步骤 2：对于所有的消息 M，对于所有的 S 盒 j 从 1 到 8。

步骤 3：对 K 从 0 到 63，对 L 从 0 到 63。

步骤 4：划分消息 M，考虑第一轮和最后一轮的第 j 个 S 盒输出的异或的一位，考虑第一轮和最后一轮的第 j 个 S 盒子密钥分别是 k 和 l（都是 6 位）。

步骤 5：分别求曲线的平均值并相减。

步骤 6：挑选尖峰最大时的 k 和 l。

步骤 7：验证找到的密钥是否正确。

可以对这 12 个猜测的位进行穷举，只需要 2^{12} 次猜测，k 和 l 中任意一位猜测错误将使得没有关联。该方法的优势是不需要精确的知道代码。

2.6.2 功耗轨迹攻击方法

功耗轨迹分析通过对一定时间范围内的电路功耗的分析，区分电路的不同状态，从而区分算法的不同步骤。攻击原理在于，执行 RSA 算法时电路在

不同时期处于不同的状态，比如存数据、取数据、算术或逻辑运算等。假设将电路的运行时间分成对应于不同电路状态的时间段，那么在每个时间段中电路功耗不尽相同。功耗轨迹分析就是通过对一定时间范围内的电路功耗的分析区分电路的不同状态，从而区分算法的不同步骤。根据这个原理，在传统的功耗攻击基础上，韩军等人[61]提出用功耗轨迹分析 RSA 的新攻击方法，新方法具有更好的可行性和有效性。

图2.8 幂指数对应比特位值是0时的功耗轨迹图形

Figure2.8 Power trace when power exponent corresponding bit is 0

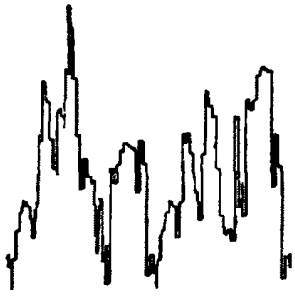

图2.9 幂指数对应比特位值是1时的功耗轨迹图形

Figure2. 9 Power trace when power exponent corresponding bit is 1

通过HSPICE仿真RSA密码协处理器，得到一个功率信号示意图。在图中有两个不同图形反复出现，结合算法的执行过程研究发现。当电路仅执行 $R = R^2 \bmod N$ 操作时，电路总功耗变化对应图2.8，当电路顺序执行 $R = R^2 \bmod N$ 操作和 $R = R * M \bmod N$ 操作时，总功耗信号变化轨迹对应的是图2.9。实际上图2.8和图2.9指示的幂指数对应的比特位值是0和1。根据这个区别，可以破解RSA算法。

针对前面提出的功耗轨迹攻击方法，一种方法就是在算法中添加多余的伪操作，从而平衡不同的操作步骤。功耗平衡是将一个周期的功耗作为整体，而实际测量的功耗是实时功耗，保证每个周期整体功耗相同不一定能够使得

周期内各处功耗相同，因此电路仍然存在安全隐患。同时伪操作没有将计算结果存储到存储器，使得功耗虽然在总体上几乎相同，但是在内部局部仍然有差异，而这个差异是可能被越来越精密的信号处理技术和工具区分开来，必须再添加数据的存储伪操作，这些都会引起功耗和运行时间的大幅度增加。

韩军等人提出在保证安全性的前提下，可以用一定概率p来添加执行伪操作，而不是全部添加伪操作，通过折中获得来安全性和性能的平衡[61]。但是研究表明，如果通过一定概率添加伪操作而不是全部添加，仍然会受到攻击。改进的算法以概率 p 来添加伪操作，假设攻击者获得 N 条功耗曲线，则可以丢弃添加过伪操作的 pN 条功耗曲线，而仅仅保留剩下 $(1-p)N$ 真实曲线，再用常规攻击方法即可攻击。

2.6.3 针对 RSA 的攻击方法

RSA是最常用的公钥密码算法之一，广泛使用在各种嵌入式密码系统，RSA同样容易受到功耗攻击。功耗攻击利用RSA密码电路的一个基本特点：密钥的每个比特不同，就会导致电路不同的运算操作。Messerges等提出了能够有效攻击RSA算法的方法，例如SEMD（Single-Exponent, Multiple-Data），MESD（Multiple-Exponent, Single-Data）和ZEMD（Zero-Exponent, Multiple-Data）[62]。他们证实，由于噪声干扰太大，SPA难以获得RSA的密钥。

SEMD攻击假设智能卡能够用秘密指数和公开指数对任意的随机值求幂。基本思想是用一个已知指数的求幂计算的功耗信号和一个未知指数的求幂计算的功耗信号进行比较。攻击者能知道这2个指数那里不同，就可以得到秘密的指数。在实际中，平方-乘积的中间结果导致功耗变化太大，直接比较不太可行，可以通过平均和相减方法来实现。

MESD攻击比SEMD攻击更强，也要求智能卡更多的假设条件。MESD攻击假设智能卡能够用一个被攻击者指定的固定指数值求幂。

ZEMD攻击与MESD类似，但是有一组不同的假设。一个假设是智能卡将用秘密的指数对很多随机的消息进行求幂计算。这种攻击不要求攻击者知道任何指数，因此称为零指数。但是攻击者需要通过脱机仿真预测平方-乘法算法的中间结果。

文献[63]提出了选择消息和内部碰撞的功耗分析方法来攻击RSA。

2.7 防御功耗攻击的方法

防御功耗攻击有两个途径，一是尽量减小功耗波动，减小功耗信息含量，即采用幅度噪声（来减小信噪比），消除功耗攻击的基础；二是尽量打乱功耗曲线与时间的关联，即时间噪声（使功耗曲线模糊）使得攻击不能成功。这两个途径都使得攻击需要更多的功耗曲线样本[64]。很多文献提出了各种不同的防御功耗攻击方法，本文对这些防御方法进行分类，认为主流的防御方法大致可以分为算法层防御和逻辑层（非算法）防御。

还有些非主流如增加片上稳流电源[65]，去耦电源[66]等电源保护措施，但是简单的电流噪声可以被信号处理技术过滤，并且增加功耗，片上电源则需要额外增加电路，提高了芯片成本。

文献[67]回顾了测试功耗分析和相应攻击的方法，包括黑盒和白盒技术。对如何生成设备安全性的证据，给出了检验合理化设计结构和评估方法。

文献[68]提出了一种独创电源智能化的片上系统（System-on-Chip, SoC）结构，可以通过控制实时支持那些屏蔽方法，电源和系统电流可以用程序预定义值。

2.7.1 算法层防御方法

算法层次的防御功耗攻击方法包括随机插入空指令或者等待状态[53, 69, 70]，消除计算中的条件分支[15, 19]和数据隐藏。数据隐藏又包括“秘密分割”[71, 72]、“复制方法”[73] “屏蔽方法”[74-76]、及随后的各种改进屏蔽方法[77-84]、以及随机变换数据的表达形式[85-87]等技术。

用随机空指令或者等待状态，程序设计者必须考虑空指令或者等待状态不被从真实的操作中区别出来。随机插入空指令打乱程序执行使能耗轨迹变化，但是通过整合技术可以重新同步能耗轨迹。消除条件分支是一种功耗平衡措施，也是避免功耗分析的基本原则；数据隐藏使得中间结果不能被直接观察，而DPA攻击要求中间结果依赖于很少的密钥和数据，因此可以防御DPA攻击[39]。秘密分割方法，复制方法大幅增加计算时间和所需要的内存；屏蔽方法在运算开始时将数据用随机数进行异或屏蔽，在进行非线性变换前将屏蔽的数据还原。

算法层的方法能够很好的防御DPA，但是他们都没有考虑更精密的高阶DPA攻击，研究表明他们不能防御高阶DPA攻击[54][88-90]。

2.7.2 逻辑层防御方法

逻辑层的防御方法不局限于特定的算法，具有普遍性。一旦某个实际的方法被提出，设计者不需要考虑对特定算法的安全性，这使得自动化设计成为可能。这类方法分为两部分：互补电路和门级屏蔽电路[91]。

逻辑层防御方法主要思想是使芯片功耗平衡来防御功耗攻击，有双轨编码的电路[92]，SABL电路[46]，循环充电SABL[93]，SDDL电路[94]，WDDL电路[94-96]，双间隔态双轨电路[97]，屏蔽双轨预充电逻辑电路[98]，低摆动电流模式逻辑[99]，功耗平衡加法器[47]；动态双轨逻辑[100]等等。

文献[101]提出了在硬件层的随机化方法。文献[102]提出了设计安全芯片的原则和概念，为了实现安全结构，提出用二元判决图（Binary Decision Diagrams, BDD）方法来设计和确定在动态电流模式逻辑（Dynamic Current Mode Logic, DCML）下最安全的结构。文献[103]提出基于全局异步局部同步（Globally-Asynchronous Locally-Synchronous, GALS）的AES算法的ASIC电路中，为了防御DPA所面临的设计挑战。接着在文献[104]中提出了用GALS系统来改进AES加密芯片防御DPA攻击的方法。

功耗平衡方法可以彻底防御功耗攻击，而且从算法级到电路级都可以采用功耗平衡方法，它的主要缺点是面积和功耗代价太大，限制了其使用。

将一个周期的功耗作为研究对象，而实际测量的功耗是实时功耗，因此保证一个周期中整体功耗相同不一定能够使得周期内各处功耗相同，电路仍然存在安全隐患。同单轨电路一样，如果信号不能够同时到达，电路产生毛刺，则还是会泄露信息。文献[105, 106]研究表明，在有毛刺的情况下，即使采用了算法级抗攻击措施，仍然会有一部分旁路信息泄露出来，仍然能够被DPA 攻击。

2.8 本章小结

本章对旁道攻击方法进行分类，介绍了电磁辐射攻击，时序攻击，故障攻击等攻击方法。建立一个旁道攻击的原理模型，分析静态互补CMOS逻辑

的结构和功耗特性，得到静态互补CMOS逻辑的功耗特性与数据的相关性，引入衡量抗功耗攻击的参数NED和NCD以及相应的计算方法。分析SPA，DPA，高阶DPA技术和新的功耗攻击技术的特点及关键技术，这些攻击方法具有通用性，能够攻击各种加密算法的芯片。由于加密算法自身特点，有些改进的攻击方法仅仅对自身算法有效，而不具有普遍性。在分析攻击方法的基础上介绍了当前的一些防御方法。

第 3 章 改进 AES 防御零值攻击

功耗攻击方法具有普遍性，与具体加密算法无关，能够对主流加密算法攻击。针对DPA攻击，有很多文献提出了各种防御方法来保护AES，如文献[72, 75, 79-82]等。他们都是基于屏蔽中间的值，例如增加一个随机数（屏蔽数）到AES中间值。

然而他们中间的文献[75]和文献[80]提出的2种方法都是一类特定（一阶）差分旁道攻击——零值攻击（zero-value attack）的受害者。零值攻击是文献[72]提出的攻击方法，能够有效攻击已经采用过屏蔽方法的AES芯片。文献[75]提出的SAMM甚至是标准DPA攻击的受害者[104]。

文献[108]和文献[109]对文献[80]提出的屏蔽方法的求逆算法进行简化，将$GF(2^4)$域乘法运算次数从8次减少到7次，降低了运算复杂度，并用硬件实现它。因为他仅仅是简化屏蔽方法的硬件实现，原屏蔽方法的缺点仍然存在，其实现的硬件将仍然能够被零值攻击。

本节研究零值攻击的方法，在此基础上提出引入随机化方法和TMM修改AES算法，用SDDL逻辑实现AES中$GF(256)$求逆运算部分的防御方法。

3.1 AES算法特点

Rijndael算法是一个迭代分组密码算法，分组长度和密钥长度可以独立指定为128比特，192比特或256比特。2001年11月它被美国国家标准和技术协会（NIST）确定为AES，以取代DES。Rijndael算法除了最后一轮，每一轮都包括字节替换（SubByte），行移位（ShiftRows），列混合（MixColumns）和轮密钥加（AddRoundKey）4个步骤。其中字节替换采用了一个8比特输入/8比特输出的S盒，S盒运算是一种非线性运算，将每个输入字节看作$GF(256)$上的元素，映射到自己的乘法逆上，全0映射到它自身。替换$GF(256)$类似于DES中的S盒，也是AES中唯一的非线性部分。

3.1.1 AES 中一些数学基础

首先AES算法中最基本的运算单位是字节，也可以看作8个比特的序列，

每个字节 b 由$b_7b_6b_5b_4b_3b_2b_1b_0$共 8 个比特组成，它是有限域$GF(2^8)$中的一个元素。一个字节的二进制数$b_7b_6b_5b_4b_3b_2b_1b_0$可以表示为系数为{0,1}中的多项式：

$$b_7x^7+b_6x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x^1+b_0$$

有限域$GF(2^8)$中最基本的两种操作是加法和乘法，在多项式表示里，加法运算可以直接用字节按位进行异或运算；乘法没有简单的以字节为单位的运算对应，它是模乘运算。

3.1.2 AES 加密算法

AES加密算法流程包括字节替换、行移位变换、列混合变换、轮密钥加操作。其轮逻辑如下：16个8比特的S盒完成字节替换，然后进行128比特的行移位变换，再经过4个32比特的列混合变换，最后与扩展出来的密钥进行异或。图3.1是AES算法主流程图。

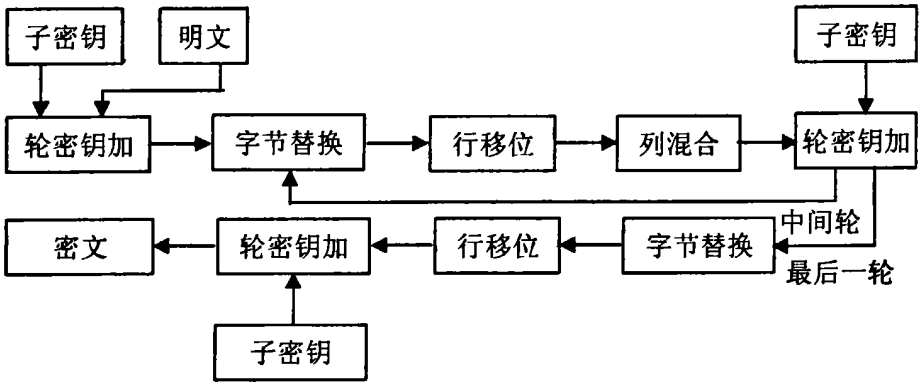

图 3.1 AES 算法主流程图

Figure3.1 The main flow of AES algorithm

AES 加密算法的总体描述和运算图示如下：

步骤 1：给定一个明文x，将 State 初始化为x，并进行 AddRoundKey 操作将 RoundKey 与 State 异或。

步骤 2：对前N_{r-1}轮中的每一轮，用 S 盒进行一次替代操作，称为 SubBytes；对 State 做一置换 ShiftRows；再对 State 做一次操作 MixColumns；然后进行 AddRoundKey 操作。

步骤 3：依次进行 SubBytes；ShiftRows 和 AddRoundKey 操作。

步骤 4：将 State 定义为密文y。

对于 AES 的每一轮，不同的变换作用于 128 比特的中间状态Y，Y 称作状态，如图 3.2，并且表示为 4*4 的矩阵$Y=(Y_{i,j})$：

Y=

Y0,0	Y0,1	Y0,2	Y0,3
Y1,0	Y1,1	Y1,2	Y1,3
Y2,0	Y2,1	Y2,2	Y2,3
Y3,0	Y3,1	Y3,2	Y3,3

图 3.2 AES 的状态 Y

Figure3.2 State Y of AES

行移位变换中，状态的第 i 行循环左移 i 个字节，其中 i=0 到 3。列混合中是以列为单位作用于状态，将每一列看作是系数在$GF(2^8)$中的多项式，乘以固定多项式$c(x)$，然后将结果模多项式x^4+1，其中$c(x)=03x^3+01x^2+01x+02$。轮密钥加变换中，每一轮的密钥按位与状态进行异或运算。

3.1.3 AES 安全分析

AES 对所有已知攻击而言是安全的，它的设计的各个方面融合了各种特色，可以抵抗各种攻击。

S 盒构造中有限域逆操作的使用导致了线形逼近和差分分布表中的各项趋近于均匀分布，这为防御差分和线性攻击提供了安全性。类似地，线形变换 Mix Columns 使得找到包含“较少”活动 S 盒的差分和线性攻击成为不可能事件（设计者将这一特色称为宽轨道策略）。

到目前为止，对 AES 还不存在快于穷举密钥搜索的攻击。即使是对 AES 减少迭代轮数的各种变体而言“最好”的攻击，也对 10 轮的 AES 无效。

3.2 零值攻击方法及防御方法

AES 的轮变换包含四种不同的变换：字节替换；行移位；列混合；轮密钥加。字节替换 Sbox 是对状态字节逐一进行置换，字节替换可逆，具有高度的非线性。字节替换由求逆变化 f 和仿射变换 g 组成，求逆变换 f 的定义为：

$$f:F_{2^n}\to F_{2^n},x\mapsto\begin{cases}x^{-1} & if \quad x\neq 0\\ 0 & if \quad x=0\end{cases}$$

仿射变换 g 的定义为：$g:F_2^n\to F_2^n,x\mapsto Ax+b$。仿射变换中增加常数 b（63H）是为了消除不动点和对应不动点。对每个字节取其在有限域$GF(2^8)$中的乘法逆，“00”被映射到它本身。

在屏蔽过的AES的第一轮，被攻击的中间变量是输入字节$Z_{1,j}=A_{1,j}\otimes Y_{1,j}$和在$GF(256)$中求逆的块输出字节$Z_{2,j}=F(A_{1,j}\otimes Y_{1,j})$。字节$A_{1,j}$由明文$P_j$和扩展密钥$K_{0,j}$得到：$A_{1,j}=P_j\oplus K_{0,j}$，因此有等式（3-1）：

$$K_{0,j}=P_j\Rightarrow Z_{1,j}=0\Rightarrow Z_{2,j}=0 \qquad (3\text{-}1)$$

乘法性屏蔽的基本问题是不能屏蔽数据中的零值字节，零值字节在被屏蔽后仍然保持不变，正是这个特性导致会受到零值攻击。另一方面，中间数据是零值在 AES 中并不能避免。

因此在本质上，对屏蔽过的 AES 和没有屏蔽过的原始 AES 一样，可以使用（一阶）DPA 攻击。对 128 位密钥的 AES 用 DPA 攻击时，穷举 1 个字节的 8 比特密钥有 256 种可能，而有 16 个密钥字节，这样功耗攻击所需要的次数是 256*16，远远小于直接攻击时的穷举法 2^{128} 次，大大降低攻击难度。不同的是，攻击者目标是全零的输入字节，或者等价的是 F 函数的全零输出。换句话说，对于$K_{0,j}$的扩展密钥的 256 种可能值中，仅仅提取$P_j=K_{0,j}$的功耗曲线用来寻找正确的密钥。而且适当的选择明文可以显著降低需要的功耗曲线数量。即攻击者只要选取合适的明文使得$P_j=K_{0,j}$，则在这种情况下的功耗将与其他情况下的功耗有显著差异。攻击者只需用 DPA 的方法从一组明文中找到这个特殊的明文，就能够破解密钥的一个字节。

文献[80]给出的抗功耗攻击实现AES硬件的方法采用修改$GF(2^8)$域求逆算法，使得输入和输出都是用同一个数进行异或屏蔽，在算法结束时进行还原操作。在修改求逆方案中，存在中间变量没有被完全屏蔽，并且满足DPA的基本前提条件：相关函数仅仅依赖于密钥中的8比特和明文的8比特。文献[72]证实，使用乘法屏蔽的AES比不使用屏蔽的AES更加容易被功耗攻击，而文献[80]提出的TMM甚至不能防御一阶DPA。根源就在于零值输入到S盒将不能被乘法性屏蔽进行有效屏蔽，而且乘法性屏蔽的弱点是内在固有的，因此不能通过修补来达到理想的安全性。

文献[110]提出了提出了一种新的最大差分功耗攻击的方法。算法对被攻击的部分明文用猜测的密钥进行变换，采用差分的方法去除噪声，比较由变换后的明文和正确密钥产生的一组功耗值，通过寻找最大功耗值得到正确的密钥。它能够以合理的攻击代价显著增强相关功耗分析攻击的效果。

为了处理零值攻击，文献[72]提出提出嵌入一个求逆操作（SubBytes的一部分）到一个大的数学结构中，以便零值映射到不同的非零值。这个方法虽然在数学表达上很好，但是代价很大，在实际应用中受限，尤其在8比特数据通道中。

文献[79]用于处理离散对数和指数表来实现SubByte操作（求逆操作是SubBytes算术描述中的一部分）。

文献[81]和文献[82]的思路与前面的方法类似，他们都假设求逆操作是一步一步运算，要么作为指数，要么在算术的混合域中。文献[81]的指数方法是适合软件实现，文献[82]的混合域方法适合硬件实现。

文献[111]提出用嵌入一个子字节操作来避开零值映射，从而防御零值攻击，但是代价太大。

Oswald 提出了一种新的综合加法性和乘法性屏蔽的方法[82]，能够有效地防御零值攻击以及其他 DPA。Oswald 方法采用了一个不同的$GF(2^8)$域求逆算法，在求逆运算过程中数据始终是加法性屏蔽的，这样就能解决文献[80]方法使用乘法性屏蔽所出现的零值攻击问题。由于 Oswald 的$GF(2^8)$域的求逆算法需要始终对数据进行加法性屏蔽，因此运算复杂度大为增加。

3.3 改进AES防御零值攻击

3.3.1 引入屏蔽方法和随机化方法

针对 AES 的零值攻击，引入屏蔽方法和随机化方法组合的模式来防御。提出将 AES 所有的轮进行屏蔽，并且第一轮和最后一轮嵌入随机化区域，其中间的运算步骤进行随机化。

采用 TMM 来保护 AES[80]，主要思想是在 AES 算法开始对消息进行屏蔽，在每一轮结束时恢复原始消息。对 AES 来说，关键是如何安全的进行$GF(2^8)$域的求逆运算，图 3.3 所示是求逆算法。

$GF(2^8)$域的求逆运算：

步骤 1：用非零的随机值Y与已经被屏蔽过的A进行乘法得到$AY \oplus XY$

步骤 2：与XY进行异或得到AY

步骤 3：求逆得到$A^{-1}Y^{-1}$

步骤 4：与XY^{-1}进行异或得到$A^{-1}Y^{-1} \oplus XY^{-1}$

步骤 5：与 Y 进行乘法运算得到$A^{-1} \oplus X$

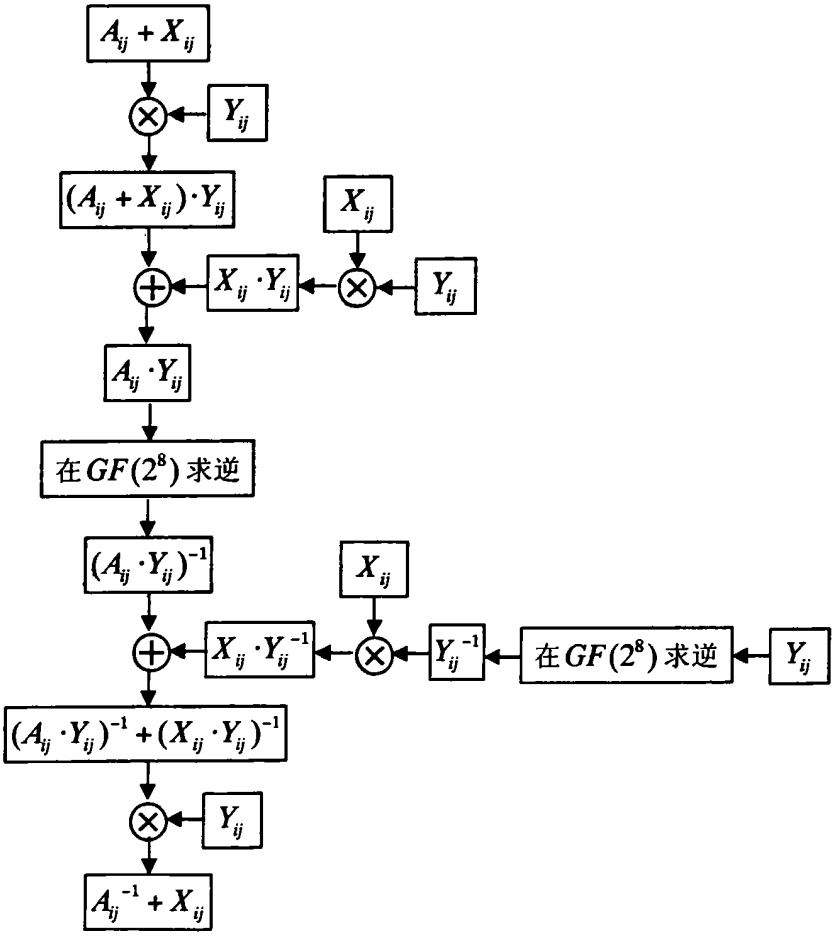

图 3.3 改进的$GF(2^8)$域求逆算法

Figure3.3 Modified $GF(2^8)$ inversion algorithm

从$A_{ij} \oplus X_{ij}$运算得到$A_{ij}^{-1} \oplus X_{ij}$，这里$A_{ij}$是 AES 运算中块$(i, j)$，$X_{ij}$是块对应的屏蔽值。图 3.4 和图 3.5 分别是原始 ByteSub 变换和改进 ByteSub 变换。

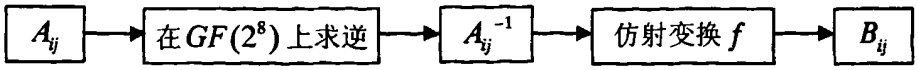

图 3.4 原 ByteSub 变换

Figure3.4 Original ByteSub transformation

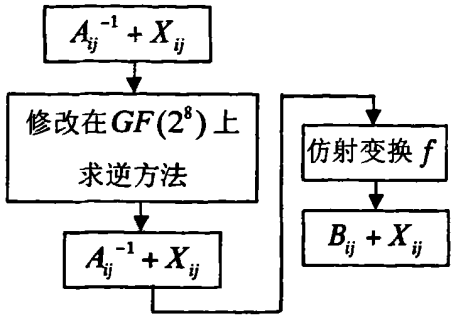

图 3.5 改进的 ByteSub 变换

Figure3.5 Modified ByteSub transformation

在 AES 算法中有几类操作可以随机化，例如轮密钥加。轮密钥加是用已经被屏蔽过的明文字节和对应的已经被屏蔽过的轮密钥进行加，这个处理顺序可以随机化，因为状态的 16 字节是分别独立处理的。同理 SubByte 也是可以随机化的操作。在列混合中，处理列的顺序可以随机化。

在 AES 算法的开始和结束时，增加轮的一部分，利用这些空的轮运行来混淆功耗曲线(称为区域 1 和区域 2)。在这两个部分运算时应用随机化方法，而在正常的 AES 轮中间，采用屏蔽方法保护。

区域 1 包括轮密钥加，SubByte 和列混合；区域 2 包括列混合，2 个轮密钥加和 SubByte。在随机化区域，屏蔽过的 AES 操作顺序随机化并且重复特定的次数。在第一个随机化区域重复的次数决定第二个随机化区域重复的次数，重复的总次数由设计者决定并且是恒定的，因此总的运行时间是恒定的。原则上屏蔽方法和随机化方法彼此独立设计，但是可以改变 AES 的 Mix-Columns 和 Shiftrow 的执行顺序来促进随机化。

3.3.2 采用 SDDL 逻辑实现$GF(256)$上求逆运算部件

SDDL 可以由普通逻辑单元库组成，不需要专门定制单元库，图 3.6 和图 3.7 分别给出了 SDDL 中与门、异或门的实现方法。逻辑门采用双轨电路的技术，无论是输入还是输出都用两根线来表示，逻辑门输出是互补的两个

输出。例如信号 A 就由 A 和 A^{-1} 共同表示，而输出 Z 也由 Z 和 Z^{-1} 表示。这样一个变量可以有 4 种不同的逻辑值（0，0）、（0，1）、（1，0）以及（1，1）。SDDL 将（0，1）和（1，0）分别用来表示逻辑 0 和 1，电路内部的逻辑 0 和 1 就变成对称，从而使得各自的功耗相同。表 3.1 是 SDDL 与门真值表。

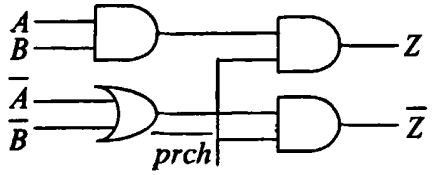

图 3.6 SDDL 与门

Figure3.6 SDDL AND gate

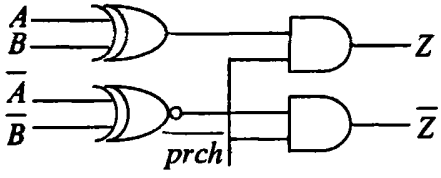

图 3.7 SDDL 异或门

Figure3.7 SDDL XOR gate

表 3.1 SDDL 与门真值表

Table 3.1 SDDL AND truth table

A	B	$\overline{A}$	$\overline{B}$	$prch$	Z	$\overline{Z}$
0	0	1	1	0	0	1
0	1	1	0	0	0	1
1	0	0	1	0	0	1
1	1	0	0	0	1	0
0	0	0	0	x	0	0
x	x	x	x	1	0	0

如图 3.8 所示，在 SDDL 中，电路的工作分为两个状态：运算状态和预充电状态。这两个状态交替更换，即在 $prch$ 上加载一个固定周期的脉冲。这样电路中变量值的变化就是 $\{(0,0)\}\rightarrow\{(0,1),(1,0)\}$ 或者是 $\{(0,1),(1,0)\}\rightarrow\{(0,0)\}$。每次翻转都只有一根信号线进行翻转，逻辑 0 和 1 达

到完全的平衡。

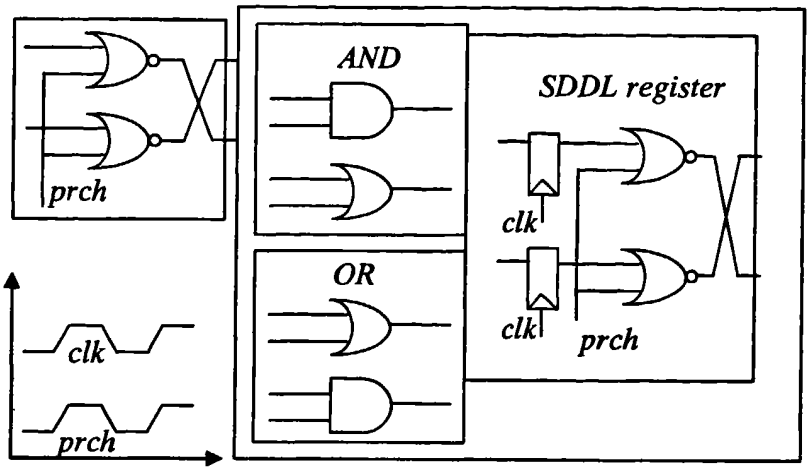

图 3.8 SDDL 触发器预充波形产生器

Figure3.8 Precharge wave generation with SDDL flap-flop's

在同步逻辑中，模块的逻辑设计可以用如 VHDL 的标准硬件描述语言描述。接下来在逻辑综合阶段用标准单元库的子集单元进行综合，子集单元包括反相器、与门、或门以及寄存器等。接下来是将综合后的静态单轨网表转换为 SDDL 网表，用 SDDL 门替代单输出门，移除反相器并且建立正确的连接。将单输出门组合在一起形成合成的标准单元库，这些单元则可以用布局工具进行布局。最后布线工具应该对每一个合成门匹配两个输出线。

将 AES 中字节变换部分采用 SDDL 逻辑实现，如图 3.9 中所示阴影模块，能够保证功耗恒定，使得零值攻击失效。

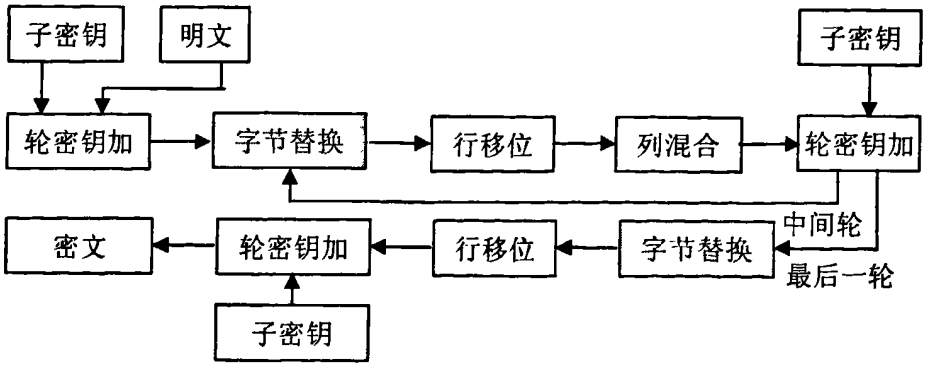

图 3.9 改进后 AES 加密算法流程

Figure3.9 Modified AES algorithm flow

图 3.10 是 AES 算法 $GF(2^8)$ 求逆的结构图，采用 SDDL 逻辑实现。任何

逻辑函数都可以只用 3 个逻辑门操作实现：非门、与门和或门。由于 SDDL 网表中所有信号都是双轨的，因此反相器是多余的。

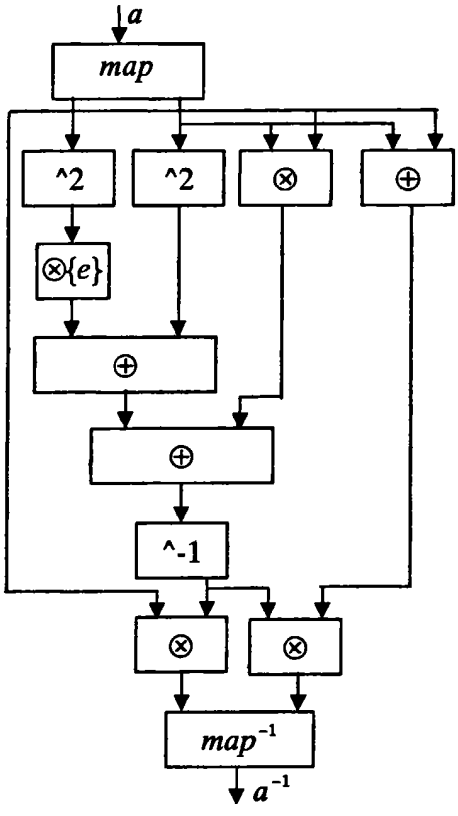

图 3.10 $GF(2^8)$ 域求逆

Figure3.10 Inversion of $GF(2^8)$

自动化设计从 VHDL 网表得到加密芯片设计，设计人员不需要特别去理解防御 DPA 的模块的实现方法，编写加密处理器代码和编写普通代码一样。在加密模块中，每一个门有独立于输入信号的恒定功耗，因此也就独立于操作被进行什么样式的编码。

3.4 安全性分析说明和仿真结果

该混合方法中，所有中间变量被屏蔽，能够防御 SPA 和 DPA 攻击。AES 执行的开始和结束使用随机化区域，这些区域中一个操作在特定点发生的概率是 $p=1/(16+4*n)$，这里 n 表示由设计者定义的块数量。二阶 DPA 对随机区域操作的攻击所得到的峰值高度将以 p 为因子下降，与标准二阶 DPA 攻击

相比，所需要的样本数是$(16+4*n)^2$。因此通过对n的选择可以使攻击变得不可行。对随机化区域外的二阶 DPA 攻击分两种情况：1）预测 MixColumns 操作后的两个中间变量；2）是预测 Mixcolumns 操作后的一个变量和随机化区域的一个变量。第一种情况下，MixColumn 操作后的任何变量都依赖于轮密钥的 32 比特，为了对 MixColumns 操作后的 2 比特进行二阶 DPA 攻击，攻击者至少需要猜测轮密钥的 32 比特，这需要太大的样本数而不可行；第二种情况下，针对他的攻击需要猜测密钥中的 32 比特，需要的样本数是标准二阶 DPA 攻击的$(16+4*n)^2$倍，在实际中同样不可行，因此能够防御高阶 DPA[112]。

在功耗分析中常采用汉明距离来进行功耗建模[113]。假定功耗变化只与输入信号变化有关，且每个比特的权重相同，可以得到如下关系：

$$P = aH(D \oplus R) + b \tag{3-2}$$

$$H(X) = \sum_{i=0}^{n} Xi \tag{3-3}$$

式（3-2）中P为功耗，a为常数；H为汉明距离函数；D和R分别为寄存器前一状态和当前状态的值；b为由噪声和其他与输入信号无关的变量引起的功耗；X为寄存器所存的数值。式（3-3）描述了汉明距离函数，即对自变量按比特求和。

为提高安全性需要付出代价。从单端输出设计变为SDDL设计，芯片在面积，时间和功耗上都有增加。使用硬件描述语言设计并实现AES加解密模

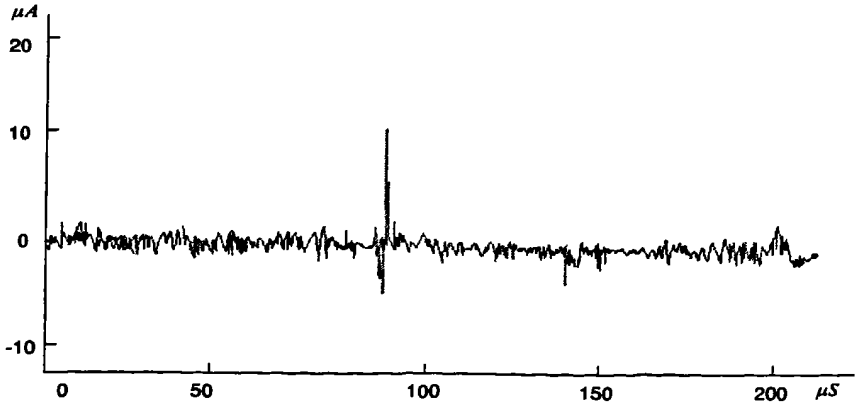

图 3.11 原始 AES 芯片的 DPA 结果

Figure3.11 Results of the DPA on original AES chip

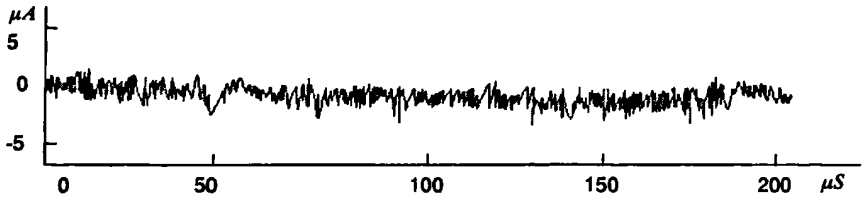

图 3.12 改进的 AES 芯片的 DPA 结果

Figure3.12 Results of the DPA on modified AES chip

块，S盒采用算术逻辑运算电路实现，采用UMC0.25 μm 工艺进行电路综合和实现。我们利用功耗分析工具PrimePower进行功耗仿真攻击，对128位密钥中的8位（第1个字节）进行攻击，采用穷举法，对于 $K_{0,j}$ 的扩展密钥的256（2^8）种可能值都猜测一遍，其余的15字节密钥位类似。

图 3.11 中原始 AES 的功耗差分曲线有峰值，其对应的密钥就是猜测正确的密钥，它不能防御功耗攻击。而图 3.12 中改进 AES 的功耗差分曲线没有明显峰值，不能得到正确的密钥，能够防御功耗攻击。

3.5 本章小结

本章指出采用屏蔽方法的AES不能防御零值攻击，需要进一步改进。提出引入随机化方法和TMM修改AES算法，介绍SDDL逻辑功耗平衡特性，生成SDDL单元库，将AES算法中 $GF(2^8)$ 求逆运算的部分用SDDL逻辑构建，使得该部分电路功耗平衡，提高防御功耗攻击的能力，能够防御零值攻击。

第 4 章 采用屏蔽技术改进 DES

没有屏蔽的加密硬件将会被DPA或高阶DPA攻击。屏蔽方法操作方便；适用于软件和硬件实现；可移植性好；以小的代价就能改变功耗和处理数据之间的相关性，能够防御一阶DPA攻击，目前广泛使用在各类算法中，也是大多数公开文献建议的防御DPA攻击的方法。屏蔽方法最初由S.Chari, C.Jutla和J.R.Rao等在文献[74]中提出，在文献[77]中深入研究。

本章研究屏蔽技术，提出改进屏蔽方法防御高阶DPA攻击，对同时存在逻辑屏蔽和算术屏蔽的算法，引入两种不同屏蔽之间进行安全转换的算法。

4.1 DES算法和安全性分析

目前广泛使用的加密方法是基于 DES，在 DES 中数据以 64 比特分组进

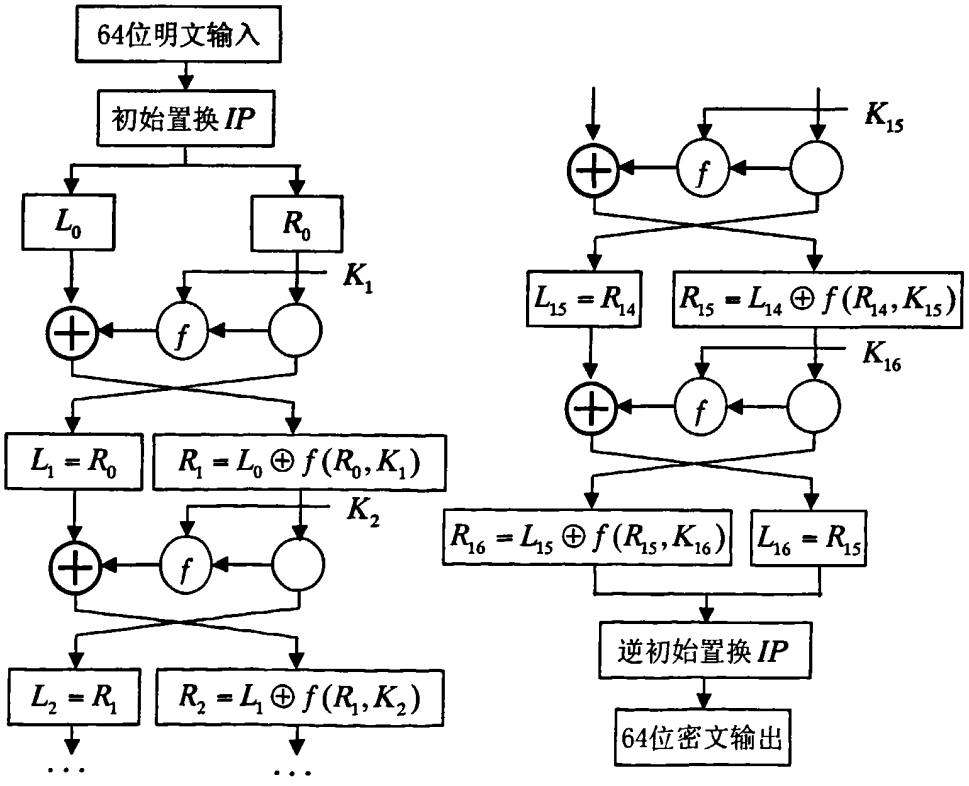

图 4.1 DES 加密算法

Figure4.1 DES encrypts algorithm

行加密，密钥长度为 56 比特。加密算法经过一系列的步骤把 64 比特的输入变换成 64 比特的输出，解密过程中使用同样的步骤和同样的密钥，如图 4.1 所示。加密与解密使用相同的密钥，它属于对称密钥体制。

DES是一个16轮Feistel型结构的对称式加解密系统。其中包括：分组长度为64比特；密钥长度为64比特，实际使用56比特，另外8比特作奇偶校验；密文分组长度也为64比特。

DES算法加密过程简述如下：对64位明文分组进行初始置换；分左右两部分分别经过16轮迭代；再进行循环移位与变换；最后进行逆变换得到密文。

4.1.1 DES 算法的基本运算

1）DES 中的初始置换 IP 与初始逆置换 IP^{-1}

对于要加密的 64 比特明文串，初始置换 IP 把原来输入的第 58 位置换为第 1 位，原输入的第 50 位置换为第 2 位，……，把原输入的第 7 位置换为第 64 位。同样的初始逆置换是以预输出作为它的输入，该置换的输出以预输出块的第 40 位作为它的第 1 位，……，而以第 25 位作为它的最后一位。

2）密码函数 f

函数 $f:\{0,1\}^{32}\times\{0,1\}^{32}\rightarrow\{0,1\}^{32}$ 的输入是一个 32 比特串（当前状态的右半部）和子密钥。密钥编排方案由 16 个 48 比特的子密钥 k_i 组成，这些子密钥由 56 比特的种子密钥 k 导出。每个 k_i 都是由 k 置换选择而来。密码函数 f 是整个加密的关键部分，它包含了四种功能：扩展函数 E，模 2 加法，S 盒运算和置换函数 P。

3）子密钥的生成过程

在 DES 中每一轮迭代都使用了一个轮密钥。轮密钥是从用户输入的种子密钥 k 产生的。实际使用密钥是 56 位，另 8 位是奇偶校验位：输出密钥 k 的每字节最后一位奇偶校验位，这些位的值使得每个字节恰好包含了奇数个 1，这样可以查到输入密钥中某个字节的错误，如图 4.2 所示是子密钥生成过程：

步骤 1：输入的密钥 k 先经过一个置换（称为“置换选择 1”）进行重排。置换结果（56 位）被当成两个 28 比特的量 C_0 与 D_0，其中 C_0 和 D_0 分别是置换结果的前 28 位和后 28 位。

步骤 2：在计算第 i 轮迭代所需的子密钥时，首先对 C_{i-1} 与 D_{i-1} 进行循环

左移，分别得到C_i与D_i。循环的次数取决于i的值：当$i=1$，2，9 或者 16，循环左移的次数是 1；否则循环左移的次数是 2。这些经过移位的值将作为下一个循环的输入。然后，以C_i D_i作为另外一个由 DES 算法固定的置换选择（称为“置换选择 2”）的输入，所得到的置换结果即为第i轮迭代所需要的子密钥k_i。

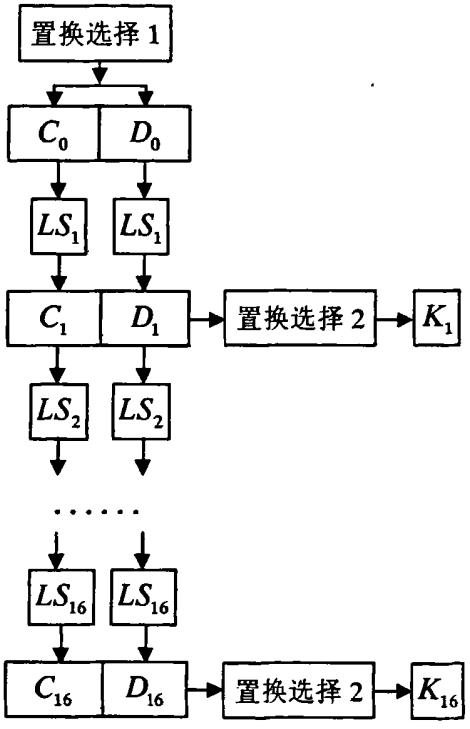

图 4.2 生成子密钥

Figure4.2 Generation sub-key

4.1.2 DES 存在的问题

1）弱密钥和半弱密钥

如果给定初始密钥k，各轮的子密钥都相同，即有$k_1=k_2=...=k_{16}$，则密钥k为弱密钥；如果存在不同密钥，可以把明文加密成相同的密文，即存在一个不同的密钥k'使$DES_{k'}(x)=DES_k(x)$，这时密钥k，k'为半弱密钥。在2^{56}个密钥的密钥空间中，弱密钥的数量极少，对于随机选取密钥来说，不足以对 DES 的安全性构成影响。

2）互补性

如果 DES 每一轮迭代运算的输入都按位取反（包括子密钥），那么迭代运算的结果也将按位取反，即 $DES_{\bar{k}}(\overline{M}) = \overline{DES_k(M)}$，DES 的互补性使得采用穷举法只要搜索一半的密钥空间，影响 DES 的安全性。

4.1.3 S 盒的特性

S盒的实现是DES算法中的关键步骤，所有其它的运算都是易于分析的线性，而S盒是非线性的，它提供了更好的安全性。S盒的设计必须非常仔细，设计S盒时必须考虑以下结构特性：

1）每个S盒有6个输入和4个输出，没有S盒的输出是输入的线性仿射函数。

2）若两个输入到同一个S盒，恰有一位相异，则输出至少有两位相异。

3）当S盒的任一位输入保持不变，其它5位变化时，所有输出的结果中0和1的总数几乎相等。

4）若两个输入到同一个S盒，在中间恰有两位相异，则输出至少有两位相异。

5）若两个输入到同一个S盒，最左边两位相异，最右边两位相同，则两个输出不同。

6）同一输入差分对应32对6比特的输入，对应于同一输入差分所产生的32个输出差分，其相同者最多不超过8个。

4.2 DES安全分析

4.2.1 对 DES 的分析方法

对于 DES 的分析方法主要包括以下三类：

1）穷举攻击。穷举攻击可用于任何分组密码，攻击的复杂性只依赖于分组长度和密钥长度。对 DES 及 Triple-DES 来说，穷举法在实际中是不可行的。

2）差分攻击。它是一种选择明文攻击方法，基本思想是：通过分析特定明文差对结果密文差的影响来获得可能性最大的密钥。差分密码分析法比较明文有某些差别的密文对，并分析明文差异在用同一个密钥加密经过不同循环时的变化传递情况，从而推算出密钥信息。

3）线形分析。它本质上是一种已知明文攻击方法，基本思想是：寻找一

个给定密码算法的有关明文比特、密文比特和密钥比特的有效的线形近似表达式，通过选择足够多的明文密文对来析取密钥的某些比特。这种方法通过异或某些明文位以及异或某些密文位得到某些密钥位的异或形式。分析收集到的明文和密文越多，线性逼近分析法攻击DES的可能性就越大。S盒有6比特输入和4比特输出，即对XOR运算，共有63（即2^6-1）和15种有用的输入输出组合。比较各个输入组合的XOR计算结果与输出组合的XOR计算结果是否有相同的概率，选取概率最大的组合方法作为某一循环的线性逼近，再将16个最佳的循环的线性逼近合成整个DES的线性密码分析。用这种方法破译DES比用差分分析方法破译DES更有效。

4.2.2 DPA 攻击 DES 方法

DES密码算法及其使用的表格、函数皆为公开数据，惟一的不公开数据仅剩主密钥，因此DES算法的安全依赖于主密钥的安全。对于攻击者来说只要破解k_i就可以倒推出主密钥中的48位，剩下的8位可用穷举法获得。DPA技术是先破解DES的子密钥k_i进而破解DES主密钥。

DES加密算法是轮迭代的处理过程，正是这种多次循环的迭代，使得芯片在运行该算法的过程中功耗呈现某种特征。攻击者可以监测并统计芯片的功耗曲线通过最大似然估计分析找出密钥。

DES算法具有16轮运算、每一轮的8个S盒均对应8组（每组6比特）子密钥、最后第16轮结果的可观察性使得第15轮部分寄存器已知等等一系列的特征。在进行针对DES算法的DPA攻击时，一般有两种策略：

1）攻击参与DES的第一轮运算的48位子密钥

2）攻击参与DES的最后一轮运算的48位子密钥

无论是猜出哪一轮的48位子密钥，均可根据子密钥运算原理再结合对另8位被舍弃的密钥的穷举，逆推出最原始的56位DES密钥。

这里以攻击参与DES的最后一轮为例加以说明[114]：

首先测出在不同明文条件下的1000次DES运算最后一轮的能量消耗。用$E1$，…，$E1000$来表示1000次运算的输出值，即密文。用$C1$，…，$C1000$来表示运算期间测出的1000条能量消耗曲线。然后关注第一个S盒中最后一轮运算的第一个输出比特，用b表示这个比特值，很容易发现b仅仅取决于密钥中的6

比特。攻击时可以对这6比特作一个猜测，用猜测的6比特和Ei来计算得到b的理论值。

根据b=0和b=1将曲线分为两类，计算曲线的平均值，记为 MC 和 MC'，从 MC 和 MC' 的波形中观察分析是否存在明显的不同，然后再猜测另外6比特密钥重复这些步骤，直到得到64对波形后，选出有明显差异的一对，这一对波形所对应的密钥就是真实的密钥。

这个方法的原理可以这样解释。由于同一电路在运行不同的数据时具有不同的功耗，因此当b值为1时电路功耗和b值为0时功耗将存在差异。b值可以由猜测的6比特和Ei计算出，即b取决于猜测的子密钥和Ei中相关位的值。而当攻击者用猜测的子密钥来计算b时，如果子密钥猜测错误，那么计算出来的b值并不反映实际电路中的运算情况，即计算出b为0时，实际电路中相应位可能为0，也可能为1；同样，计算出b为1时，实际电路中相应位仍然可能为0，也可能为1。既然b值取决于猜测的子密钥和Ei中相关位的值，而Ei是随机输入，则b的值也将是随机的为0或1。即为0或1的概率相等，为50%。这种情况下根据b值来划分曲线，产生的效果是将实际电路中的功耗曲线进行随机划分为两类，这两类功耗特征完全是将错就错的随机特性（有时本该被归到1那类的功耗可能被归为0那类，反之也是），大量归类后特征相互抵消，统计后几乎没有差别。如果子密钥猜测正确，那么结合Ei计算出来的b值和实际电路中的相应位相同。这时如果b值为0，则实际电路中相应位为0；如果b值为1，则实际电路中相应位为1。这种情况下根据b值划分实际电路的功耗曲线时，可以把不同特征的功耗曲线分开，即实际电路中相应位为0的功耗曲线为一类，实际电路中相应位为1的为另一类。功耗曲线的分类将真实地反映b值为1和0之间的差别。采样越多，就对功耗差别特征的体现贡献越多，猜对子密钥就立刻体现出比猜错子密钥明显的功耗差别。

DPA关键点在于消除了算法级噪声，SPA则没有消除。原因在于DPA在分析过程中仅仅定位一位数据（如L16中的一位），即使在同一个密钥的情况下，其他的位的变化和这位都是独立的。当输入的明文数据是随机的，电路与该位数据不相关的部分都可以认为近似随机变化，差别基本为0，进行统计后几乎没有差别。差分功耗分析可以对微小的功耗差别进行分析，分析能力较SPA要强许多。

4.3 屏蔽方法防御DPA

屏蔽技术是利用一个随机数 r 对需要屏蔽的关键信息进行异或处理，把关键数据变成随机数。由于 r 是未知的，非法用户无法获得被屏蔽的关键信息，可以防止分析关键数据。

文献[55]采用的屏蔽方法是对子密钥进行屏蔽，在屏蔽的子密钥和明文异或进入S盒之前将子密钥恢复。每一轮运算的子密钥与功耗曲线之间的相关曲线发生改变，从而影响攻击者进行功耗分析，提高了抗功耗攻击的能力。

4.3.1 屏蔽方法在 DES 算法中的使用

DPA攻击方法中划分函数D的值受密钥、明文/密文的影响，另外DPA的对象主要是使用固定密钥进行加解密操作的加密系统。因此设计防御DPA的改进DES模块时，主要考虑密钥对划分函数D的影响。为了使划分函数的值和功耗曲线之间相关性尽可能地变小或为0，在DES算法中对密钥进行屏蔽。

DES运算中对加法和乘法，可以用算术屏蔽；除了加法和乘法，其他的基本操作很容易用逻辑屏蔽过的数据操作，并且得到屏蔽的输出，因此可以用屏蔽策略。图4.3是针对DES的屏蔽方法。

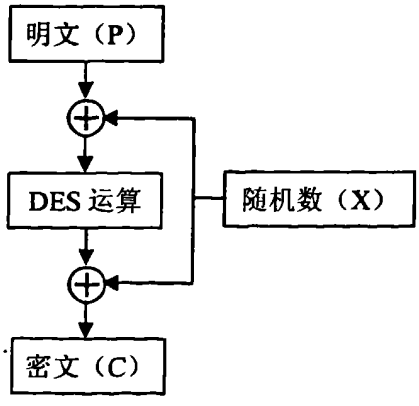

图4.3 屏蔽DES算法

Figure4.3 Masking DES algorithm

屏蔽技术被用来保护设备防御DPA攻击，他利用一个随机数r来对硬件的输入和输出进行处理。在使用屏蔽的例子中，芯片用中间变量（依赖于密钥中的b比特）来执行一些运算时，不直接和b计算，因为这会使b暴露给DPA攻

击。它是通过2步完成，首先和随机比特r运算；然后和屏蔽过的比特（r+b）运算，用屏蔽过的中间值作为输入继续进行余下的计算。在这种情况下，仅仅知道r和r+b中的一个，对攻击者来说没有任何用处。

文献[55]提出DES_Mask算法，是采用屏蔽技术对DES运算中的明文和密钥进行屏蔽。其基本原理：在明文输入时，首先用一个随机数r对子密钥k_i（$1 \le i \le 16$）进行屏蔽（异或操作）；在进入S盒之前消除随机数（还原操作）；然后经过S盒运算继续后面的运算步骤；最后得到和标准DES一样的计算结果。他利用屏蔽方法实现了能够防御DPA攻击的DES_DPA加密芯片，并且对其进行了仿真。

4.3.2 异或屏蔽和加法屏蔽方法

DES算法中屏蔽操作有两种类型，一种为逻辑屏蔽，用位的异或操作运算；一种为算术屏蔽，用2^{32}模的加法运算。以随机数r和要屏蔽的字x为例来说明这2种类型，操作后的结果是x'，其中r是由随机数硬件发生装置产生的，x是未经屏蔽的值，x'是屏蔽后的值[55, 115]。

1）仅仅包含算术运算单元，加法屏蔽

输入：(x,r)，$x'=x+r$

输出：(A,r)，$x=A+r$　　假定 C 为随机数 1 或 0

步骤 1：$B=C\times r$

步骤 2：$D=C\times x$

步骤 3：$A=B+D$

步骤 4：$A=A-B$

步骤 5：$A=\overline{(A-B)\oplus C}$

容易看出来：$A+r=x$

2）仅仅包含逻辑运算单元，异或屏蔽

输入：(x,r)：$x'=x\oplus r$

输出：(A,r)：$x=A\oplus r$　　假定 C 为随机数 1 或 0

步骤 1：$B=C\oplus r$

步骤 2：$A=C\oplus x$

步骤 3：$A=A\oplus B$

容易看出来：$x \oplus r = \bar{x} \oplus \bar{r}$

4.3.3 异或屏蔽和加法屏蔽之间的相互转换

由于 DES 算法中存在逻辑运算和算术运算，而对这两种运算屏蔽的方法不同，需要两种屏蔽之间相互转换。为了避免转换时可能出现没有屏蔽过的关键信息而导致信息泄露，转换方法必须是安全的，必须能够防御 DPA 攻击。很多文献给出了安全转换的方法[55, 115-118]：

1）从异或屏蔽到加法屏蔽的转换

输入：(x,r)：$x' = x \oplus r$

输出：(A,r)：$x = A + r$　　假定 C 为随机数 1 或 0

步骤 1：$B = C \oplus r$

步骤 2：$A = C \oplus x$

步骤 3：$A = A \oplus B$

步骤 4：$A = A \oplus B - B$

步骤 5：$A = A + C$

步骤 6：$A = A \oplus C$

2）从加法屏蔽到异或屏蔽的转换

输入：(x,r)：$x' = x + r$

输出：(A,r)：$x = A \oplus r$　　假定 C 为随机数 1 或 0

步骤 1：$B = C \times r$

步骤 2：$D = C \oplus x$

步骤 3：$A = D + B$

步骤 4：$A = (A - B) \oplus B$

由于 C 的不确定性，攻击者不能确定运算时的中间变量是 x 或者是 $\bar{x}$，而且 x 和 $\bar{x}$ 都与随机数 r 相关，因此 DPA 攻击不能成功。

4.4 采用变型的屏蔽方法改进DES算法

本文研究发现，文献[55]提出的DES_Mask，应用的屏蔽方法在数据进入S盒之前就消除随机数，不能防御后来提出的高阶DPA攻击，是二阶DPA攻击的受害者。为了完全屏蔽密钥，本文引入TMM来防御DPA攻击，基本思想是

使得每一轮的输出与输入是用同一个随机数进行的屏蔽，用一个随机数对所有数据进行异或。在数据进入S盒之前不恢复密钥，继续保持屏蔽状态进入S盒，由于S盒是非线性的，为了保证S盒的输出将来有机会消除随机数还原得到正确的数据，需要修改原始S盒。

标准的DES算法采用8个不同的S盒，因此修改的DES算法也要对应的8个修改的S盒，每个S盒需要256位寄存器。S盒的修改与随机数有关，根据每次加密的随机数生成新的S盒，这样随机性提高，但是资源消耗较大。

TMM 与屏蔽方法的主要区别是：TMM 在算法的开始和结束时对消息进行屏蔽，其他都不变，在算法结束时恢复预期的值；屏蔽的方法必须关注算法的每一步屏蔽情况，需要知道在固定步骤屏蔽的值（例如在轮或是非线性部分结束时）。如图 4.4 所示是采用屏蔽方法时修改 S 盒。

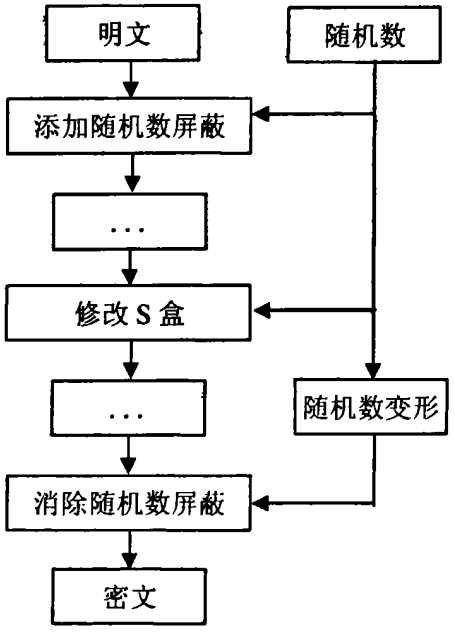

图4.4 采用屏蔽方法时修改S盒

Figure4.4 Modified S-box with masking method

用 DES 算法加密 64 位的消息 M，选择一个 64 位的屏蔽值 X，在算法开始之前用 X 和 M 进行异或，这样实际上是以 M⊕X 作为开始的值。

修改后的 S 盒记为：

$$SM-Box(A)=S-Box(A\oplus X2)\oplus P^{-1}(X1_{0-31}\oplus X1_{32-63}) \qquad (4\text{-}1)$$

式（4-1）中 P^{-1} 是 S 盒之后的逆置换。

应用屏蔽方法的问题在于算法的非线性部分，而且对称加密算法的安全性本质上是依赖于非线性部分。DES 唯一的非线性部分是 S 盒，在初始置换 IP 之前用 X 进行加法屏蔽，在用屏蔽时修改 S 盒，这样后面才能够恢复屏蔽的值。在置换 FP 之后，将屏蔽消除得到正确结果。

可以提前把修改后的 $SM-Box(A)$ 盒计算出来存储，即采用查找表法，优点是速度快，缺点是占用资源。也可以实时计算 $SM-Box(A)$ 盒，但是这样导致加密速度慢，性能下降。

4.5 安全性分析说明和仿真结果

采用屏蔽方法后的DES算法可以防御功耗攻击。以第i轮为例，已知 L_i，R_i，k_i 和 r_i 分别是数据左边部分，右边部分，子密钥和随机数，运算中间值 $f(R_i,k_i)=P(S(E(R_i)\oplus k_i))$。采用屏蔽方法后的DES算法中子密钥 k_i'，可以知道 $k_i'=k_i\oplus r_i$，运算中间值是 $f_i=E(R_i)\oplus k_i$，和 $f_i=E(R_i)\oplus k_i'$，容易得到 $f_i'=f_i\oplus r_i$。即 f_i' 和 f_i 异或后是随机数，因此其相关系数是0。

在上述中提出了几种掩码步骤中，由于C的不确定性，在该过程中攻击者无法获得中间变量，而且由于随机数:对数据的掩码改变了操作数和功耗之间的相关性，因此功耗攻击的难度增大，提高了加密系统的安全性。

在DPA析攻击中，攻击者利用被攻击芯片的假设模型来估计其旁道输出[23]。根据2.5.1节中的旁道攻击的原理模型，采用功耗攻击分别对原始DES芯片和采用改进防御方法的DES芯片进行模拟攻击，计算芯片理论功耗和模型的相关系数。即攻击者将用假设模型算出芯片运行的某个时刻的功耗信息与实际的功耗信息进行相关性分析，得出二者之间的相关系数。用 Ti 表示第 i 次实际测量到的旁道信息，用 T 表示某一组测量结果的集合。用 Pi 表示第 i 次假设模型估计的结果，用 P 表示某一组估计结果的集合。则可以得到：

$$C(T,P)=\frac{E(T\times P)-E(T)\times E(P)}{\sqrt{Var(T)\times Var(P)}} \qquad (4\text{-}2)$$

式（4-2）中 $E(T)$ 表示某一组测量结果的期望，$Var(T)$ 表示某一组测量结果的方差。如果某一组测量结果的相关系数远远大于其他组的相关系数，则说明在这组假设模型中所使用的密钥是正确的[109]。

芯片功耗的变化主要是内部寄存器值的变化所导致，根据DPA原理进行

模拟攻击。统计某个时钟周期前后寄存器数值变化的个数即汉明距离，作为理论模型的功耗值。进行攻击时，假定进入第一个修改后的S盒的6位明文是 Ti，6位子密钥为 Ki（$1 \le i \le 8$），根据 Ti 和 Ki 可以确定S盒的4位输出。具体的功耗攻击分析方法如下：

步骤1：随机选择1000个明文，即 $1 \le k \le 1000$，用 Ti 和 Ki 进行运算，可以得到输出值的变化导致寄存器变化的情况，通过其汉明距离得到理论模拟的功耗 T，它是一个1000*1的矩阵。

步骤2：S盒的输入子密钥 Ki 是6位，寄存器的6比特共有64个可能值；穷举所有可能的密钥，重复步骤1，和随机明文运算，计算寄存器对应比特在运算前后的汉明距离，估算模型功耗信息。得到的1000*64的假设模型功耗信息矩阵 Pk。

步骤3：将模型功耗信息和理论功耗进行相关性评估，得到相关性系数。根据式（4-2），对 P 中每一行的数据与 T 进行相关系数求值运算，求出理论功耗 T 与模型功耗 P 之间的相关度。

步骤4：相关度最高的一行数据，其功耗信息 P 所对应的猜测密钥就最可能是正确密钥。相关性系数越大，则密钥猜测正确的可能性越大，相关性最大的点对应密钥正确的可能性最大。

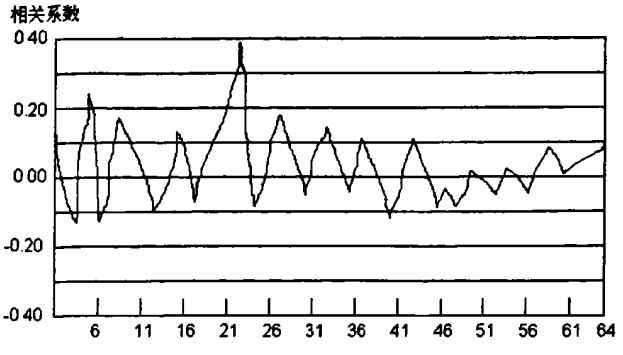

图4.5 攻击普通DES算法的结果

Figure4.5 Results of analysis DES algorithm

采用1000个随机明文进行仿真攻击实验，图4.5是普通DES的功耗与数据的相关性示意图，从图中可以看出在密钥序列22的地方，其相关系数最大，即理论功耗和模型功耗相似程度最大，其对应的密钥最可能是正确的密钥，

DPA攻击普通DES获得成功。图4.6是改进DES的功耗与数据的相关性示意图（两个图的刻度不一样），其相关性很小。

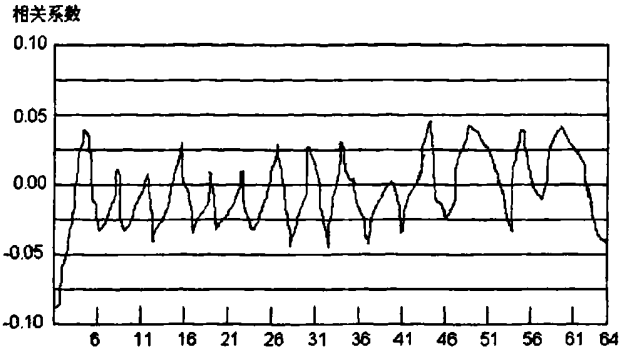

图 4.6 攻击改进的 DES 算法的结果

Figure4.6 Results of analysis modified DES algorithm

对采用改进屏蔽攻击后的设计中，相关系数绝对值几乎都在0.05以内波动，没有表现明显的相关性，不能找出对应的密钥。

在实际攻击芯片时，由于有其他的噪声以及测量误差，其所需要的功耗样本比理论上的攻击样本要多。因此本文的方法能够提高防御DPA攻击能力。

4.6 本章小结

本章提出改进的屏蔽方法，在数据进入非线性部分之前不恢复密钥，而是修改算法的非线性部分（DES算法中是S盒），使得数据在经过非线性变换后仍然能够恢复。算法中同时存在异或屏蔽和加法屏蔽，引入异或屏蔽和加法屏蔽之间相互转换的具体方法，使得算法中的敏感数据不以明文出现，能够完全屏蔽。对该算法的安全性分析表明可以防御新提出的攻击。

第 5 章 算法层和逻辑层结合防御 DPA 攻击

事实和理论都证明，屏蔽技术可以防御 DPA，但不能防御高阶 DPA，仍然是高阶 DPA 攻击的受害者[53, 54]为了防御高阶 DPA 攻击，一些研究人员进行了相关研究。Akkar 和 Giraud 等提出了一个新的方法——UMM，并将其应用到 DES 中[60]。文献[107]研究表明，该方法并不能防御高阶 DPA，随后提出了新的防御方法。文献[88, 119]发现其新的防御方法仍然不能防御高阶功耗攻击，其随后提出了进一步改进 UMM 的防御方法（下文称为 Lv 防御方法）。Lv 防御方法可以防御高阶 DPA，但是资源要求较大。

本章研究 UMM 及改进方法，根据 SABL 逻辑的结构和原理，利用其功耗平衡特性，设计功耗恒定的基本逻辑单元，并通过仿真得到逻辑单元的特性参数。提出一种算法层和逻辑层结合的改进方法，设计能够防御高阶 DPA 攻击的芯片，比现有方法所需资源少。

5.1 采用UMM改进DES算法

秘密分割方法、屏蔽方法、TMM 等能够防御 DPA 攻击，但是都不能防御高阶 DPA 攻击。Akkar 和 Giraud 提出 UMM，试图通过修改 DES 算法来防御高阶 DPA 攻击[60]。

5.1.1 独特屏蔽方法

UMM方法大致可以分为2个步骤：

步骤1：得到屏蔽的轮

产生一个32比特的随机数α，基于原始DES中S盒函数，自定义2组S盒S_1和S_2如下：

$$\forall x \in \{0,1\}^{48},\ S_1(x) = S(x \oplus E(\alpha))$$

$$\forall x \in \{0,1\}^{48},\ S_2(x) = S(x) \oplus P^{-1}(\alpha)$$

这里E是扩展变换，P^{-1}是S盒之后的逆置换。

定义f_{ki}，$f_{1,ki}$和$f_{2,ki}$函数如下：

f_{ki}函数由扩展变换E，第i轮子密码ki，S盒以及P置换构成，记为f；

将 f_{ki} 函数中 S 盒分别用 S_1 和 S_2 代替得到 $f_{1,ki}$ 和 $f_{2,ki}$，分别记为 f_1' 和 f_2'。可以看出 $f_{1,ki}$ 是从屏蔽过的值得到没屏蔽的值，$f_{2,ki}$ 则从没屏蔽的值得到屏蔽过的值。用 f_{ki}，$f_{1,ki}$ 和 $f_{2,ki}$ 函数可以得到屏蔽或者没屏蔽的5种类型的轮：

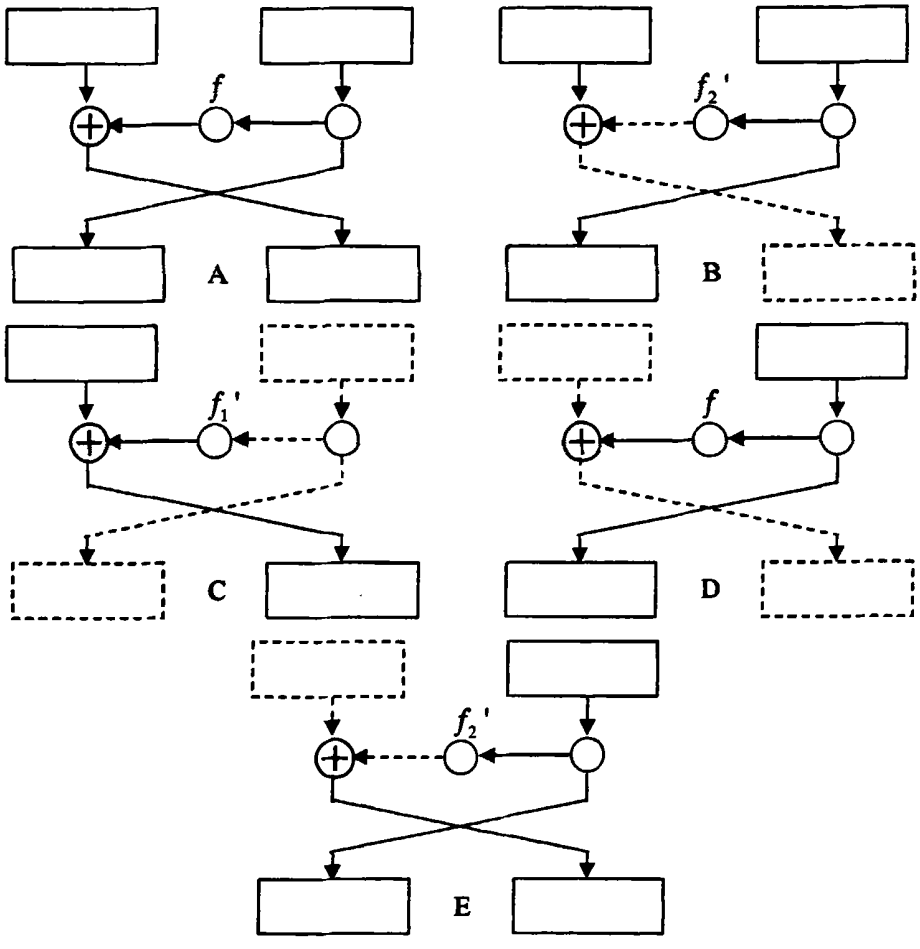

图 5.1 正常的轮（A）和屏蔽过的轮（B-E）

Figure5.1 Normal round(A) and masked rounds(B-E)

图 5.1 是 5 种类型轮结构图，虚线是屏蔽过的，实线是没有屏蔽的。

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 $f_{2,ki}$ 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 $f_{1,ki}$ 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 $f_{2,ki}$ 函数，输出时左右两部分都是没屏蔽的值。

步骤 2：用屏蔽的轮组成 DES

DES的合法轮序列由图5.2所示的有限状态自动机构成。为了防御DPA攻击，所有依赖少于36比特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*。

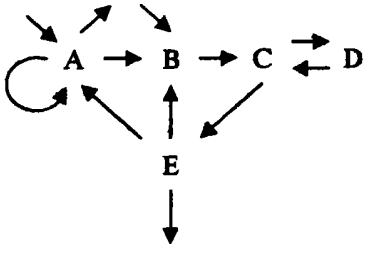

图 5.2 自定义 5 种类型轮的合法序列

Figure5.2 Valid sequence for five kinds of user-defined rounds

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。

5.1.2 对 UMM 的攻击及第一次改进

所有合法的轮序列中第二轮都是 C 类，S 盒的输出是没有屏蔽的，而且在与消息的左边部分异或后仍然是没有屏蔽的。在异或之后结果通过 E 类或者 D 类是没有屏蔽的，对于通过 D 类甚至 S 盒的输出和 P 排列都是没有屏蔽的。第二轮的输出没有屏蔽这个特点导致该 DES 轮序列将会受到攻击[107]。

攻击采用选择明文的方法，主要思想是恢复两个没有被保护的中间值，然后解一个包含这 2 个中间值的等式得到密钥比特。

攻击分 3 步如下：

步骤 1：选择一组消息 M_i，使得 $R_{0,i}$（消息 M_i 经过初始变换后的右边部分）是一组任意的恒定值 R_0，而 $L_{0,i}$ 则是随机。

对第二轮的 S 盒的输入执行一阶 DPA 攻击。因为第二轮的 S 盒的输出是

没有屏蔽的；第一轮的S盒的输出是未知但是恒定，结合这 2 个输出，可以猜测第二轮的密钥。第一轮的 S 盒的输出是：

$$\delta = K_2 \oplus E(P(S(K_1 \oplus E(R_0)))) \tag{5-1}$$

步骤 2：用另一组任意的恒定的值R_0'执行一阶 DPA 攻击，第一轮的 S 盒的输出是：

$$\delta' = K_2 \oplus E(P(S(K_1 \oplus E(R_0')))) \tag{5-2}$$

步骤 3：异或式（5-1）和（5-2）中得到的值δ和δ'：

$$\delta \oplus \delta' = (K_2 \oplus E(P(S(K_1 \oplus E(R_0))))) \oplus (K_2 \oplus E(P(S(K_1 \oplus E(R_0')))))) \tag{5-3}$$

K_2值消失了，并且由于E，P是线性函数，进一步简化式（5-3）得到：

$$\delta \oplus \delta' = E(P(S(K_1 \oplus E(R_0)) \oplus S(K_1 \oplus E(R_0')))) \tag{5-4}$$

式（5-4）中已知R_0和R_0'，对K_1的 6 位子密钥可以用穷举法得到它的值。

针对这种攻击，改进的方法是增加定义一个f_{3,K_i}函数，修改S_3使得：

$$\forall x \in \{0,1\}^{48} : S_3(x \oplus E(\alpha_1)) = S(x) \oplus P^{-1}(\alpha_1) \tag{5-5}$$

引入式（5-5）后，改进的第 2 轮S输出为：

$$S(E(P(S(K_1 \oplus E(IP(M)_{32-63}))) \oplus IP(M)_{0-31} \oplus \alpha_1) \oplus K_2) \tag{5-6}$$

同前面类似，将式（5-6）中的 E 展开可以得到：

$$S(E(P(S(K_1 \oplus E(IP(M)_{32-63})))) \oplus E(IP(M)_{0-31}) \oplus E(\alpha_1) \oplus K_2) \tag{5-7}$$

结合式（5-5）中S_3的定义，得到第 2 轮S输出值为：

$$S(E(P(S(K_1 \oplus E(IP(M)_{32-63})))) \oplus K_2 \oplus E(IP(M)_{0-31})) \oplus P^{-1}(\alpha_1) \tag{5-8}$$

输出值（5-8）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。

5.1.3 对改进后的 UMM 攻击及第二次改进

在上面的改进方法中，第1，2轮的S盒输出是用相同随机数屏蔽的，文献[88]根据这个特点对其提出攻击方法，下文称为Lv攻击方法。通过异或第1，2轮的S盒输出，消除UMM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。

攻击分 3 步如下：

步骤 1：第 1 轮 S 盒的输出：$S(K_1 \oplus E(IP(M)_{32-63}))P^{-1}(\alpha_1)$ （5-9）

步骤 2：第 2 轮 S 盒的输出：

$$S(E(P(S(K_1 \oplus E(IP(M)_{32-63}))))\oplus K_2 \oplus E(IP(M)_{0-31}))\oplus P^{-1}(\alpha_1) \quad (5\text{-}10)$$

步骤 3：异或第 1，2 轮 S 盒输出（即异或值（5-9）和值（5-10））得到：

$$S(E(P(S(K_1 \oplus E(IP(M)_{32-63}))))\oplus K_2 \oplus E(IP(M)_{0-31}))\oplus S(K_1 \oplus E(IP(M)_{32-63})) \quad (5\text{-}11)$$

随机值 $P^{-1}(\alpha_1)$ 在值（5-11）中消失了，同样可以用选择明文攻击：固定 IP 右边的32比特为一个任意的随机值，让左边32比特随机输入，可以得到值（5-11）中 $S(E(P(S(K_1 \oplus E(IP(M)_{32-63}))))K_2$ 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。改进UMM没有很好的屏蔽最前2轮和最后2轮，这4轮泄露的能耗特征容易被攻击，它们是防御高阶DPA攻击的薄弱环节。

针对 Lv 攻击方法，文献[88]提出第二次改进防御方法，下文称为 Lv 防御方法。

首先产生 3 个 32 比特的随机数 X_1，X_2，X_3；基于原始 S 盒定义 6 组新的 S 盒，针对不同的轮对应不同的 S 盒，具体如下：

1，6，11，12 轮：$\overline{S}(x) = S(x) \oplus P^{-1}(X_1)$

2，5，10，13 轮：$\overline{S}(x)$ 使得 $\overline{S}(x \oplus E(X_1)) = S(x) \oplus P^{-1}(X_2)$

3，4 轮：$\overline{S}(x)$ 使得 $\overline{S}(x \oplus E(X_2)) = S(x) \oplus P^{-1}(X_1 \oplus X_2)$

7，16 轮：$\overline{S}(x) = S(x) \oplus P^{-1}(X_3)$

8，15 轮：$\overline{S}(x)$ 使得 $\overline{S}(x \oplus E(X_3)) = S(x) \oplus P^{-1}(X_2)$

9，14 轮：$\overline{S}(x)$ 使得 $\overline{S}(x \oplus E(X_2)) = S(x) \oplus P^{-1}(X_1 \oplus X_3)$

根据这些新的 S 盒定义新的 f 函数，然后用新的 f 函数代替 DES 中原来的 f 函数，起到保护 S 盒输出的效果。

5.2 功耗平衡逻辑

很多方法试图在结构层或者算法层消除供电电流的波动，然而这些方法都不能真正有效防御 DPA 以及派生出来的攻击方法，因为电流波动产生的根源在于逻辑层。Kris Tiri 等人在 2002 年第一次提出具体应用 SABL 来防御 DPA，SABL 组合了双轨逻辑和预充电逻辑的思想，是一种动态差分逻辑电

路[46]。运行时功耗几乎完全相等，功耗独立于信号跳变，与输入数据及顺序无关，彻底消除了功耗攻击的物理基础。可以用在各种加密电路中有效防御 DPA 攻击，但是需要设计一个全新的单元库，同时硬件资源需求较大。

使用功耗平衡的 SABL 来实现电路，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；类似的有动态电流模型逻辑，它的缺点是晶体管大小与输出电容有关，甚至取决于最后的布局布线；而且它需要复杂的时钟延迟网络，不同的逻辑深度需要不同的时钟延迟[120-121]，这些导致设计难度增加。

文献[100, 122]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，来提高防御 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。在设计试验 DES 算法中，DES 算法的基本部件被执行，在不考虑布局寄生效应的情况下，晶体管级的仿真表明其有优异的安全性。

5.2.1 SABL 结构

SABL 有两个特点：1）它是一个动态和差分逻辑，因此每个周期有一个跳变，并且独立于输入值和序列。2）在跳变时刻它充放电所有的内部节点电容和平衡输出电容[46, 123]。

SABL 逻辑门由触发器构成，为了实现基本的门，保留触发器灵敏放大器部分，而用差分下拉网络替换掉原来的输入差分对，一般结构如图 5.3 所示。它是一种动态双轨互补逻辑，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；当时钟上升为高电平后电路处于求值阶段，不管输入信号是什么，双轨输出一个维持高电平，一个降为低电平。

图5.3中 M_1 管与 M_2 管的作用是对电路进行预充电，这两个PMOS管与 M_4 管共同负责逻辑门的预充电、求值阶段转换。在预充电阶段，逻辑门的内部节点全部预充到高电平。差分下拉网络DPDN（differential pull- down network）决定着逻辑门的基本功能，在求值阶段，它为两个交叉耦合反相器中的一个提供一条接地通路。这个特定反相器的输出转换为低电平，这使得另一个反相器的输出维持在高电平。

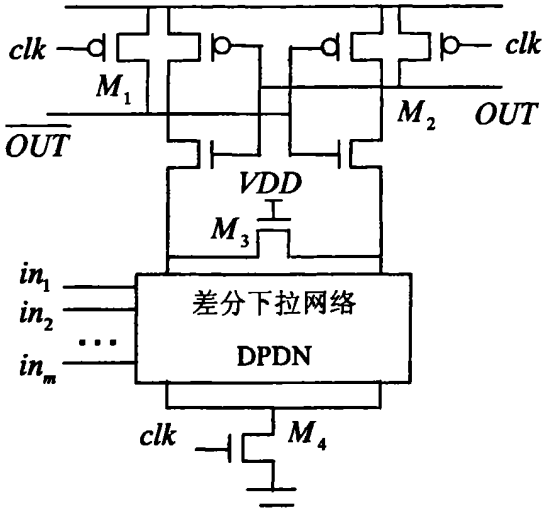

图5.3 SABL逻辑门结构图

Figure5.3 Structure diagram of SABL logic

5.2.2 SABL 逻辑特性

对于一般的SABL逻辑门，不管输入信号的值是多少，整个下拉网络中所有的寄生电容都进行放电，在下一次预充电阶段需要对所有的寄生电容进行充电。逻辑门每次消耗的能量都基本相同，极大地减小了运算数据与功耗之间的相关性。scCMOS的NED超过为80%，而SABL低于3%[46]。因此SABL逻辑门能够更好的起到防御功耗攻击的作用。

电路的所有SABL单元都连接到时钟信号，并且同时预充电，这导致很高的电流峰值。而且SABL单元需要的硅片面积至少是普通CMOS的2倍，并且有很大的延迟[64]。除了逻辑单元，单元之间的互连线也要用专门的平衡方法布线，来达到能耗统一。SABL组合了双轨逻辑和预充电逻辑的思想，他需要设计和描述一个全新的单元库，同时能耗太大。

5.3 定制功耗恒定标准单元库

功耗平衡电路包括几个方面：1）在采用高层实现安全措施的同时，对于电路中其他防御功耗攻击方法薄弱的运算单元进行功耗平衡设计；2）功耗平衡，高性能，低代价的运算电路一般要求进行全定制设计；3）功耗平衡的基本运算单元具有通用性，在不同密码芯片设计中调用可以提高设计效率。

基于 SABL 设计功耗恒定的逻辑门标准单元库：先确定逻辑单元的各项参数指标，使用 CosmosSE 设计逻辑图；在用 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。标准单元的通用设计流程及所用的软件工具如图 5.4。

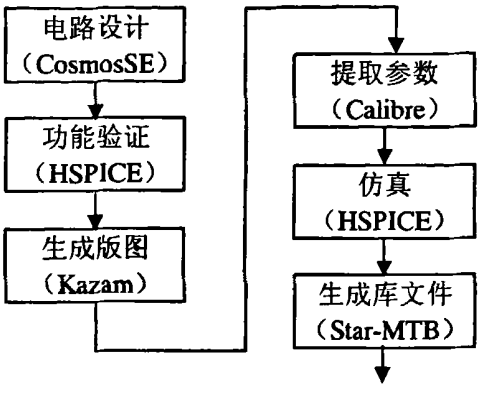

图 5.4 标准单元的设计流程

Figure5.4 Design flow for standard cell

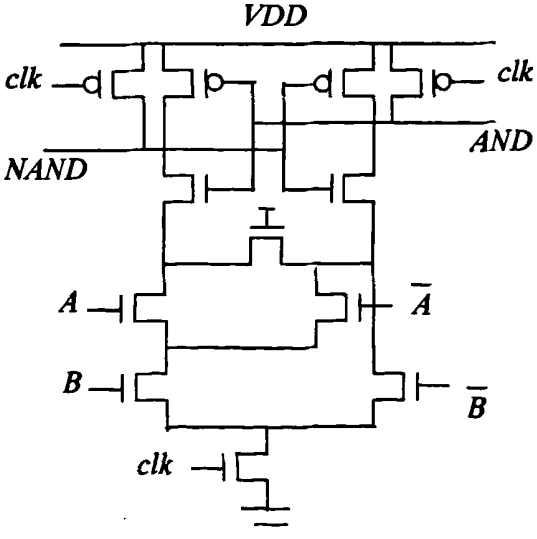

图 5.5 SABL 逻辑两输入与非门结构图

Figure5.5 2-input NAND gate structure diagram with SABL

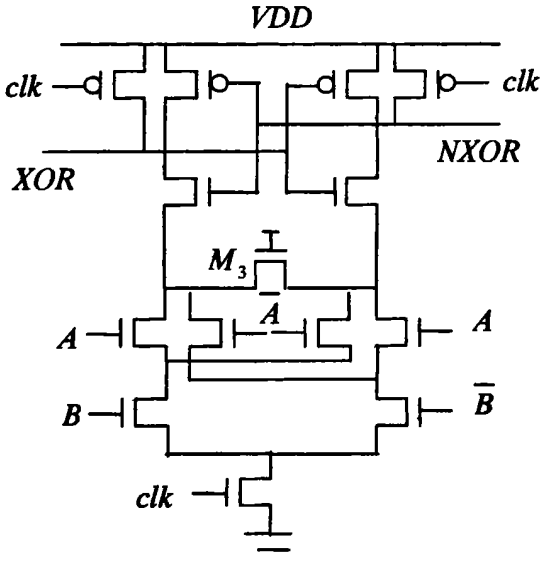

图 5.6 SABL 逻辑两输入异或门结构图

Figure5.6 2-input XOR gate structure diagram with SABL

采用前面的设计方法构建的 SABL 基本逻辑门，图 5.5 和图 5.6 是与非门和异或门的结构图。

5.4 用SABL实现S盒的原因

加密算法运算的不同时期所执行的操作不同，功耗泄漏的信息也不同，选择那一部分功耗信息进行功耗分析对攻击成败至关重要。选择得合理将能够减少所需样本数，降低攻击难度；反之可能需要太多的的样本，以至于不能成功。

S 盒是DES中唯一的非线性部件，不论取 *S* 盒输出的哪一位作为划分函数 *D* 的目标位，这一位不仅对 *S* 盒输入对应位值敏感，而且对输入的其它位值的变化也敏感。这种良好的扩散性能，保证了划分函数 *D* 期望值的相对独立性，而其他的线性部分无法做到这一点。*S* 盒的特点说明防御线性攻击的性能指标和防御DPA的性能指标是矛盾的，即 *S* 盒非线性度越高，防御线性攻击能力越强，同时防御DPA的能力越弱。从直观上看，差分功耗分析利用的是功耗的差异来寻找密码。而 *S* 盒起扩散作用，很小的输入变化导致很大的输出变化，放大了输出数据的差异，而这同时放大了功耗的差异，因此适合作为DPA攻击的目标，选择 *S* 盒作为功耗攻击目标是合理的。

AES 中第一轮运算中 *S* 盒的输出字节是输入字节的函数，而输入字节本身是对应得明文和密钥的按位和，这就满足了前文提到的执行 DPA 攻击的前提条件。DPA 攻击方法对非线性函数的攻击效率更高，所以字节替换函数的输入就是最有效的 DPA 攻击的目标。此外轮密钥加函数执行数据和密钥的按位异或，这是在 AES 算法中唯一直接操作数据和密钥的函数，如果攻击成功就可以从中获得密钥子集，因此也可以作为攻击目标。但由于异或操作是线性运算，所以对轮密钥加函数的输出做 DPA 攻击需要采集更多的能耗数据。

对 *S* 盒的保护至关重要的，由功耗平衡逻辑特性可以知道，SABL 逻辑门能够起到抗功耗分析攻击作用；同时 UMM 方法的几次改进，都没有完全屏蔽 *S* 盒的输出信息，因此将 *S* 盒用 SABL 实现是合理的。

5.5 UMM与SABL结合防御高阶差分功耗分析

用防御功耗分析的运算硬件单元实现敏感的或易受攻击的操作，可以弥补其他安全措施的不足，或者降低对于其他安全措施的安全度要求。在本文方法中，功耗平衡电路用来实现关键电路，其他部分和上层的实现安全用算法保证。

Lv 防御方法从算法层考虑提出防御方法，认为屏蔽 16 轮防御高阶 DPA 需要满足 5 个条件，进而给出了防御方法所需的最少资源。本文认为 Lv 防御方法的 5 个条件实际上是对所有轮进行有效屏蔽，使得攻击者不能消除随机数，而实际上可能屏蔽 16 轮中的部分轮就能够保证 DES 的安全。DES 运算从第三轮开始，参与计算的密钥数达到 36 位，超过 DPA 攻击所要求的少于 32 位，这表明并不需要对所有的轮进行屏蔽，因此 Lv 防御方法不一定是保护 DES 安全应用的最小代价。可以结合使用其它方法来保护关键的第 1，2，15，16 轮，而不是 16 轮都用屏蔽方法保护，不屏蔽所有的轮可以减少硬件需求。

将第 1，2，15，16 轮这 4 轮用 SABL 逻辑门来实现，提高防御重叠攻击的能力，使 Lv 攻击方法失效，不需要满足他提出的 5 个条件，同样可以达到防御效果。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。

提出采用 SABL 逻辑结构，设计功耗平衡单元库。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，提出能够抵抗高阶 DPA 攻击的 DES 芯片结构，使芯片能够防御任意阶 DPA 攻击。并采用半定制设计流程实现芯片电路。

首先建立模块所需要的所有单元，然后用这些单元进行布局布线得到模块。内部和外部单元布线的寄生电容不仅仅导致性能的显著下降，特别是输入输出延迟增大和能耗增加；而且导致每个跳变时刻整体电荷的改变，如果两个差分输出信号遇到不同的寄生电容。因此需要特别关注每一个单元的布局，尽量平衡它的固有内部和外部电容，单元之间的布线在相同环境下进行，这确保对于其他金属层的寄生电容是相似的。而且在长的邻近线之间的交叉耦合也要用屏蔽来解决，屏蔽付出的代价是能耗和面积增加。

5.6 安全性分析说明和仿真结果

容易看出，DES 中每一轮的 S 盒输出都是用某个随机数屏蔽过的，因此可以防御 SPA 和一阶 DPA。

从 n 阶 DPA 攻击方法知道，为了实施 n 阶 DPA 攻击，攻击者需要知道 n 个中间变量，以便知道很少的密钥比特位（实际中一般少于 32 比特），可以使得攻击者确定对于 n 变量的函数，是否 2 个输入值（对应 2 个输出值）得到相同的值。由于 E 的扩散特性和 P 排列以及 S 盒，被高阶 DPA 攻击的中间变量的可能值将是下面这些组合：最前 2 轮的 S 盒输出；最后 2 轮的 S 盒输出；第一轮和最后一轮的 S 盒输出；第二轮和最后一轮的 S 盒输出；第一轮和第十五轮的 S 盒输出；最前面 2 轮和最后面 2 轮的 S 盒输出。其他的组合，使得密钥数超过 32 位，不满足 DPA 攻击的基本假设。上面这些可能被攻击的组合中，每一个异或值都是一直被随机数屏蔽，并且这些随机数每轮加密都会改变，于是攻击者不能正确地判断两个输入值（对应两个输出值）是否得到相同的值。同时采用 SABL 实现最前两轮和最后两轮，其功耗平衡使得攻击者不能获得功耗特性曲线。因此改进的 UMM 方法能够防御高阶 DPA 攻击。

本文实现 SABL 逻辑的功耗恒定标准单元库，然后用该单元库设计实现 DES 算法中的 S 盒，并对其功耗进行测试和分析。对 S 盒的 Spice 网表进行

模拟，得到一段电流特征曲线如图 5.7 所示，其功耗曲线几乎相同，其特性与预期相吻合，与 scCMOS 相比，其功耗与输入信号的相关性大大降低。

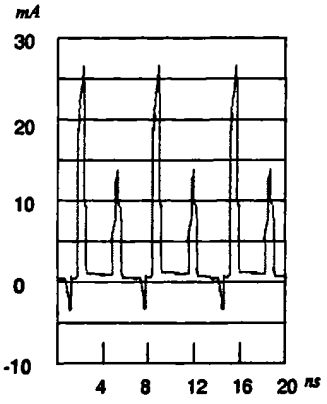

图5.7 SABL逻辑S盒仿真电流曲线

Figure5.7 Simulated current trace of SABL S-box

5.7 本章小结

本章研究表明UMM及几次改进方法不能防御高阶DPA。在其基础上提出算法层和逻辑层组合的防御方法，改进UMM算法；研究SABL逻辑特性，设计功耗平衡SABL逻辑单元库，半定制设计流程，并指出用SABL实现 S 盒的原因。安全性分析和仿真实验表明改进算法提高了防御高阶DPA攻击的能力。

第 6 章 防御功耗攻击的 DES 芯片设计

分析现有 DES 芯片实现方法，根据 DES 算法的特点，设计能够防御高阶 DPA 攻击的 DES 芯片。修改原始 S 盒，增加 1 个随机数和 2 组 S 盒。采用 SABL 实现 DES 芯片关键部分模块；采用 CMOS 实现非关键部分模块，最后构成整体 DES 芯片。设计实现芯片时考虑智能卡的限制，在一些指标的选择上进行折中，采用部分流水结构。对其进行性能仿真分析并与现有芯片进行分析比较，芯片能够实现加解密，能够防御高阶 DPA 攻击，比以前的方法节省资源，满足实际的应用。

6.1 基本DES芯片结构

对于当前使用的 DES 芯片实现主要有下面三种结构：

1）循环递归式结构[124, 125]

循环递归式结构如图6.1所示，在这种结构中仅使用一组逻辑电路和寄存器去建立DES算法，相同的逻辑电路需要重复16次才完成DES算法，这种结构大大节省硬件资源和芯片面积。但是在一个时间点只能有一组数据输入电路，新的一组数据的输入需要在电路完成16轮的操作以后，减少了数据的吞吐量。比如一轮数据处理的时间是n，则整个DES算法的处理时间是16n。如果对芯片的资源利用率有很高的要求，而对数据处理速率没有很高要求的话，这种结构是很合适的。

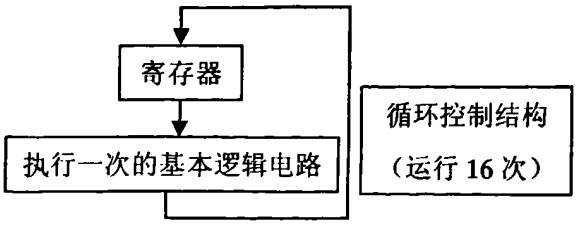

图 6.1 循环递归运算结构图

Figure6.1 Circular recursion computation structure diagram

2）完全流水线结构

为了使DES算法能够最快处理数据，DES的16轮运算能够单独地同时进

行运算，这样16轮运算就形成了一个16段的流水线。16个不同的输入能够同时输入到流水线中去，这种结构的DES算法是由16段组成，每一段由一个寄存器和一个基本逻辑块组成，每段都可以单独地处理输入数据，寄存器用于存储本段需要处理的数据。

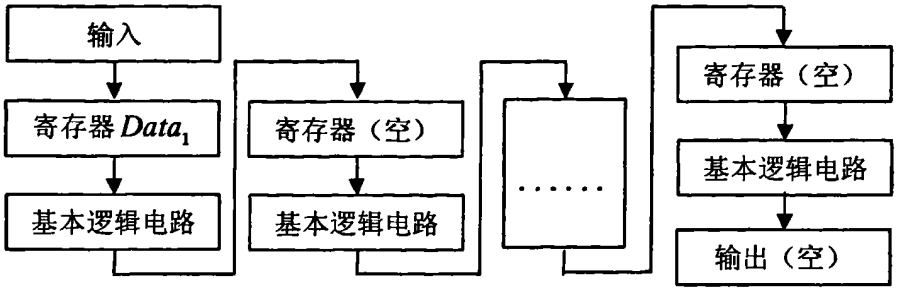

图6.2 运算的第一个周期

Figure6.2 First cycle of computation

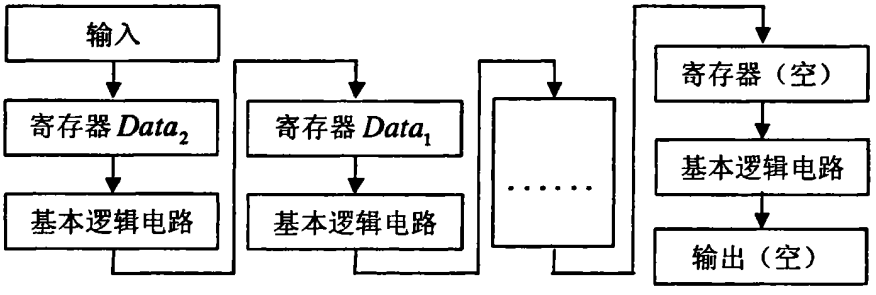

图6.3 运算的第二个周期

Figure6.3 2th cycle of computation

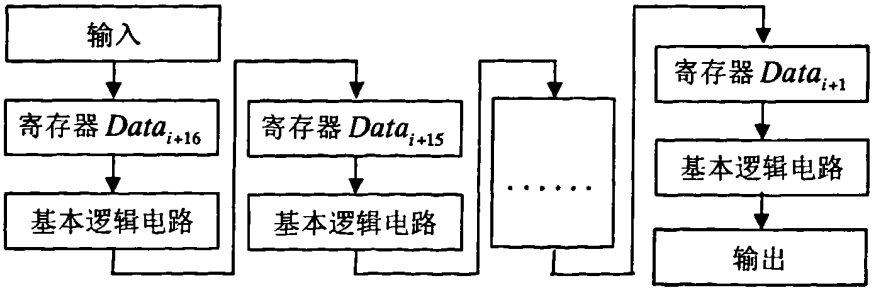

图6.4 运算的第i个周期

Figure6.4 i cycle of computation

首先 $Data_1$ 被输入到寄存器1，在被寄存器1的基本逻辑块处理完以后，输出被送到寄存器2中去。与此同时 $Data_2$ 被送到寄存器1中去。那么就有两个

输入：寄存器2的输入$Data_1$，寄存器1中的输入$Data_2$，这样就形成了流水线。随着处理过程的进行，$Data_3$被输入到寄存器1，……，当所有寄存器都有数据后，处理并行度最大。图6.2，图6.3和图6.4分别是完全流水结构运算的第一个周期，第二个周期和第i个周期。

在这种结构中，一组数据的处理时间和一轮的处理时间大致相等，数据处理速度得到极大的提高。但是采用这种结构，资源的占用要比递归式的结构高得多。只有在对速度要求很高的场合才采用此结构。

3）混合式结构

这种结构是循环递归式结构和完全流水线结构的混合体。也就是说这种DES结构既包含递归式结构电路，也包含流水线式结构电路。混合式结构既能达到一个好的资源利用率，也能达到一个相当高的数据吞吐量，在寻求资源利用率和数据处理速率之间平衡，是一个折中的方法。

这三种结构都没有考虑防御功耗攻击，文献[55]提出的防止功耗分析的DES-DPA硬件设计则考虑了功耗攻击。出于性能价格比、减少硬件开销的考虑，在设计 DES-DPA 模块时，仅对子密钥信息使用屏蔽技术，其中每执行一轮 DES 算法，随机数发生器的初始值（种子）就改变一次。在具体设计实现阶段，考虑到时间、面积的折衷，DES_D PA 模块选择 4 段结构。

6.2 功耗平衡电路实现DES关键模块

定义逻辑输出翻转为(q_{i-1},q)，相应的功耗则是$E(q_{i-1},q)$。在组合电路中，输入信号常常是在不同时刻到达逻辑门的，这导致电路的输出在一个周期内翻转多次，也就是常说的毛刺。假设逻辑门的输入在 k 个不同时刻到达，那么逻辑门的功耗可以用公式表示如下：$E=(E_0,E_1,...,E_t,...E_{k-1},E_k)$，其中$Ei$是在时刻$i(v_t)$和时刻$i+1(v_{t+1})$之间逻辑门的功耗。

功耗平衡是解决功耗攻击问题的根本途径，但功耗平衡电路比普通电路往往实现复杂、性能低、面积大。采用组合方法的优点是在已有实现安全措施的基础上进一步提高安全性，同时又尽量少的使用功耗平衡电路。采用半定制设计能够得到优化的电路，由于单元可以重复利用，克服了全定制电路设计周期长的缺点。

S盒采用 SABL 逻辑门实现的 DES 轮记为 SABL_S，其功耗平衡使得不

管逻辑门的输入信号与信号序列是什么，密码模块都消耗几乎相等的功耗，可以提高防御 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，用此门电路实现第 1，2，15，16 轮，得到功耗平衡的 DES 轮。图 6.5 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。

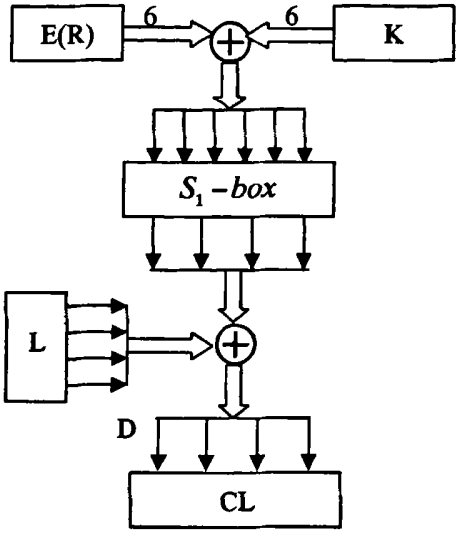

图 6.5 第一个 S 盒的运算模型

Figure6.5 First S-box computational model

将 S 盒用 SABL 逻辑构成，随机输入数据进行仿真，对 S 盒的 Spice 网表进行模拟得到 NED 值为 2.32%。

6.3 用UMM保护部分DES轮

S 盒采用CMOS逻辑门实现的DES轮记为CMOS_S，用CMOS_S实现DES的第3至14轮变换模块，S盒的功耗与输入数据及顺序有关联，其功耗非恒定将被DPA攻击，结合UMM方法屏蔽来保护。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，使得经过S盒（或修改过的S盒）后能够得到所需的数据。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组额外的 S 盒，用修改过的 S 盒替代原始 S 盒，得到5种类型轮。由于UMM轮的独特性，DES中第3至14轮有多种合法轮序列，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组成不同的轮序列。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。

第 1，2，15，16 轮用 SABL 逻辑实现，其功耗恒定，功耗特征与输入没有关联，不用考虑 UMM 方法中第二轮 S 盒输出有没有被屏蔽，即可以防御选择明文攻击。同理也不用考虑第一轮和第二轮的 S 盒输出是否用相同的随机数屏蔽，不需要满足 Lv 防御方法提出的 5 个条件，因此可以大大减少硬件的需求。

6.4 组合方法构建的DES芯片硬件实现

设计过程分以下几步：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 DES 轮；采用 UMM 方法定义 5 种类型轮；按照合法轮序列构建整体 DES 芯片；对芯片进行功耗模拟，证实防御功耗攻击的能力。

由于电路采用不同类型的逻辑构成，一般的逻辑综合工具、布局布线工具不支持抗功耗分析攻击逻辑单元的特殊结构，传统的设计流程不完全适用。本文采用半定制设计流程，将 SABL 逻辑类型融入普通的 EDA 工具设计流程中，在满足设计要求情况下，充分利用现有工具提高设计速度。设计流程如图 6.6 所示，其中网表转换步骤是将逻辑综合得到的单轨逻辑门级网表替换成动态双轨逻辑门级网表。

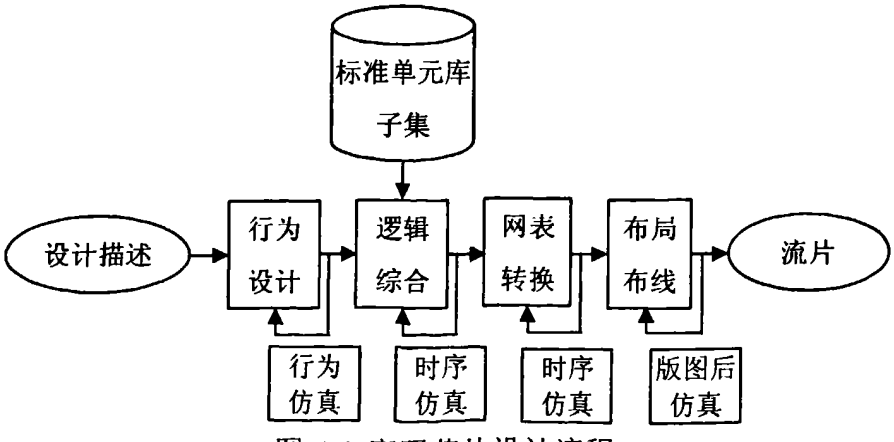

图 6.6 密码芯片设计流程

Figure6.6 Cryptograph chip design flow

因为双轨逻辑的所有信号都是差分的，如果一个信号经过反相后连接到一个逻辑门的输入端，只需要将这个信号的差分互补信号直接连接到逻辑门的输入端即可，门级网表中的反相器可以消除。

将网表中的反相器消除后，再对其它逻辑门进行替换操作，可以将综合后的门级网表看作字符串文本，用脚本程序对门级网表进行字符串处理，得到相应的双轨逻辑门级网表。

将两种轮结合起来，考虑到实现 DES 芯片运算速度、面积和成本的约束，将部分模块复用。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 $IP-(BC)_{SABL\_S}(DCDCEBCDCDCD)_{CMOS\_S}(CE)_{SABL\_S}-IP^{-1}$，$(BC)_{SABL\_S}$ 表示 UMM 方法中的 B 类和 C 类用 SABL 逻辑实现，其他与此类似。实现 DES 的关键模块电路结构如图 6.7 所示，省略了其他辅助模块。

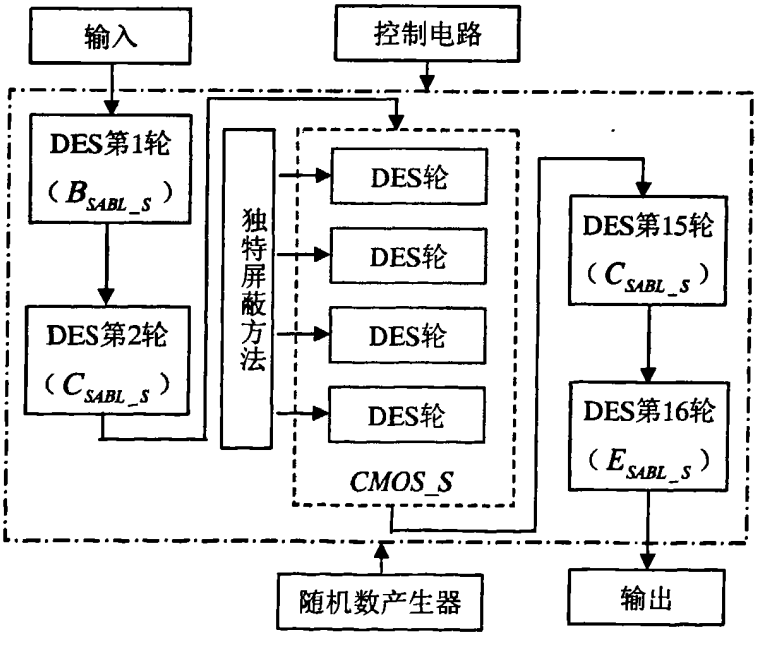

图 6.7 综合方法实现 DES 结构图

Figure6.7 DES structure implemented by combination approach

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。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可以减少流片次数，缩短设计周期和降低成本。

6.5 性能仿真测试和比较

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轮和第15，16轮，其功耗变化幅度几乎为0。不管UMM方法中第二轮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，它都可以防御功耗攻击。提高了这4轮防御选择明文及重叠攻击的能力，弥补UMM的薄弱环节，使Lv攻击方法失效。理论证明过程如下所述。

根据组合方法实现加密电路的描述，下面的引理和其推论可以证明本文设计的电路可以防御功耗攻击。证明过程方法与文献[96]所述类似。

引理1：组合方法实现的电路可以防御DPA攻击。

证明：根据功耗攻击方法描述，设DPA攻击的划分函数是$z_j = D(K,C_j)$，其中k是猜测的密钥的一部分，C_j为第j组样本对应的密文。攻击者根据z_j的值将功耗样本分为两个子集S_1和S_0。假设z_j产生时刻是t，则样本子集S_1和S_0在时刻t的功耗平均值的差为$\Delta E(t)$[126]：

$$\Delta E(t) = [\sum_{j=1}^{m} z_j P(j,t) / \sum_{j=1}^{m} z_j] - [\sum_{j=1}^{m} (1-z_j) P(j,t) / \sum_{j=1}^{m} (1-z_j)] \qquad (6\text{-}1)$$

式（6-1）中m为样本数，$P(j,t)$表示第组功耗样本在时刻t的值，$P(j,t)$表达式如下：

$$P(j,t) = \sum_{i=1}^{M} E_i(t) = \sum_{i=1}^{M} [P_i(t) + \varepsilon_i] \qquad (6\text{-}2)$$

将式（6-2）代入式（6-1）就可得到$\Delta E(t)$的平均值为0，就是说不管密钥k猜测的是否正确，$\Delta E(t)$都没有偏差，没有峰值出现，因此DPA攻击失败，可以防御DPA攻击。

证毕。

推论1：组合方法实现的电路可以防御高阶DPA攻击。

由引理1知道，采用SABL实现的DES最前2轮和最后2轮的关键轮，其功耗与输入没有关系，攻击者不能得到划分函数的划分，也就不能高阶DPA攻击。采用CMOS实现的中间其他轮，其中间值所依赖的密钥位数是36位或56

位，大于DPA攻击所要求的32位，不满足DPA攻击的条件。因此总的电路可以防御高阶DPA攻击。

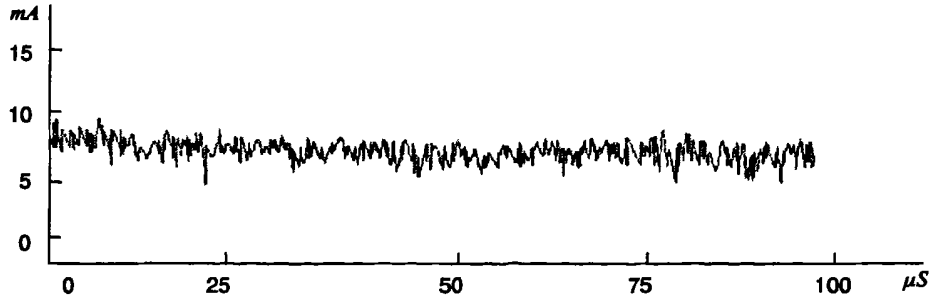

图6.8 组合方法构建的DES的功耗曲线

Figure6.8 Power trace of DES constructed with combition method

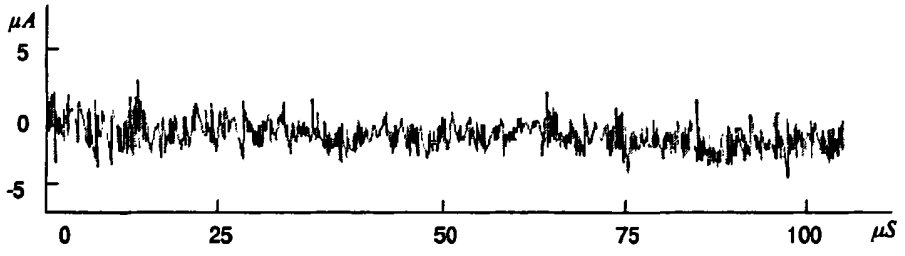

图 6.9 组合方法构建的 DES 的差分功耗曲线

Figure6.9 Differential power trace of DES constructed with combition method

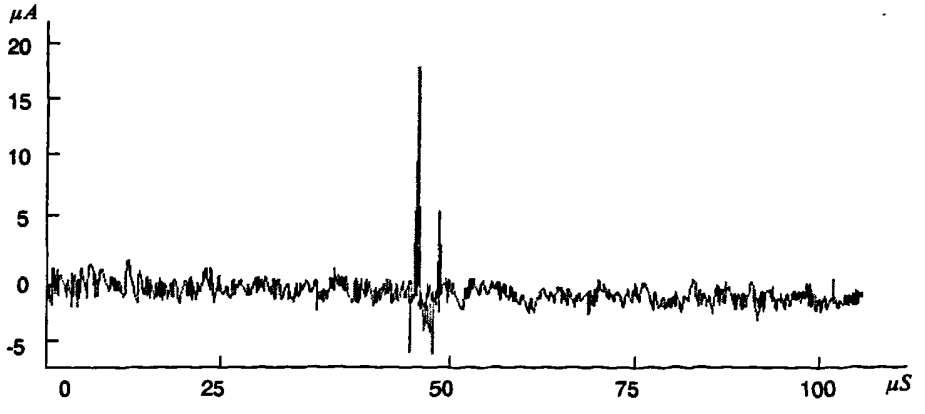

图 6.10 CMOS 构建的 DES 的差分功耗曲线图

Figure6.10 Differential power trace of DES constructed with CMOS

图6.8是组合方法构建DES的功耗示意图；图6.9是采用SABL结构的差分功耗曲线，差分电流很小；图6.10是CMOS结构的差分功耗曲线，可以看到有一个差分功耗极大的峰值。利用功耗分析工具PrimePower进行功耗仿真攻

击，本文设计的芯片功耗与输入数据相关性降低，其NED值为2.32%，采用普通CMOS逻辑的电路NED值超过80%。

实现防御高阶 DPA 攻击的 DES 时，UMM 方法需 2 组额外 S 盒，在 ST19 元件工作频率为 10MHz 时，实现一次加密时间是 $38ms$[60]；Lv 防御方法加密时间是 $67ms$；本文方法加密一次约耗时 $70ms$。Lv 防御方法需 6 组额外的 CMOS 结构 S 盒，3 个随机数；本文需 2 组额外的 CMOS 结构 S 盒以及用 4 组 SABL 结构 S 盒，1 个随机数，比 Lv 防御方法节省资源，几种方法实现的 DES 比较如表 6.1 所示。

表 6.1 不同方法实现的 DES 芯片比较

Table6.1 Comparison of DES chip with differential methods implementing

实现 DES 的方法	随机数个数	额外 S 盒组数	采用的逻辑（未模块复用）
UMM	2	2	16 轮 CMOS
改进的 UMM	2	3	16 轮 CMOS
Lv 防御方法	3	6	16 轮 CMOS
本文的方法	1	2	4 轮 SABL，12 轮 CMOS

表 6.2 不同逻辑实现的 DES 芯片比较

Table6.2 Comparison of DES chip with differential logic implementing

实现 DES 的逻辑门	功耗	面积	加密一次时间（模块复用）
CMOS	16p	16a	$38ms$
SABL	30.56p	28.8a	-
本文的方法(CMOS 和 SABL)	19.64p	19.2a	$67ms$
本文的方法/SABL	64.27%	66.67%	约 $70ms$

文献[46]给出了分别用 SABL 和 CMOS 实现 S9-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，不考虑其它次要因素的情况下，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 6.2 列出了不同逻辑门实现 DES 的功耗和面积。

6.6 本章小结

本章分析目前 DES 硬件加密结构的特点和实现方法，根据 DES 算法的特点，设计能够防御高阶 DPA 攻击的 DES 芯片。分析现有 DES 芯片实现方法，修改原始 S 盒，增加 1 个随机数和 2 组 S 盒，采用部分流水结构。采用 SABL 实现 DES 芯片关键部分模块，提高该部分电路防御重叠攻击的能力，弥补独特屏蔽方法的薄弱环节，对 S 盒的 Spice 网表进行模拟得到 NED 值为 2.32%；采用静态互补 CMOS 实现非关键部分模块，减少功耗和面积，最后构成整体 DES 芯片。设计实现芯片时考虑智能卡的限制，在一些指标的选择上进行折中，采用部分流水结构实现智能卡。对其进行性能仿真分析并与现有芯片进行分析比较，芯片能够实现加密/解密，运算速度与现有方法相当，能够防御高阶 DPA 攻击，比以前的方法节省资源，有一定的先进性。

结　论

功耗攻击目标是使用固定密钥的芯片，它是攻击加密芯片的一个重要方法，攻击效果好，实施成本低，并且非常难被监测，尤其是高阶DPA攻击能力更强，更加难以防御。本文对现有的功耗攻击及防御方法进行研究，特别是DPA和高阶DPA攻击技术进行研究，针对其特点及关键技术，提出相应的防御方法。

研究内容包括AES的零值攻击防御方法；改进屏蔽方法防御DPA攻击；改进UMM算法，设计具有防御高阶DPA攻击能力的DES芯片，并进行仿真验证，解决加密系统的功耗分析问题。对新出现的专门针对具体加密算法有效的攻击方法，也进行了研究并提出相应的防御方法。通过上述工作，取得以下创新性研究成果：

1）基于随机化方法和变形屏蔽方法修改了AES算法。引入随机化方法和TMM修改AES算法，同时将AES算法中$GF(2^8)$求逆运算的部分用SDDL逻辑构建。理论分析表明，攻击本文方法所需要的样本数是标准二阶DPA的$(16+4*n)^2$倍，通过选择n可以更进一步提高防御能力，使得攻击不可行。采用UMC0.25um工艺进行电路综合和实现，利用功耗分析工具PrimePower进行功耗仿真攻击。对128位密钥中的8位（第1个字节）进行攻击，其余的15字节密钥位类似。采用穷举法，对于$K_{0,j}$的扩展密钥的256（2^8）种可能值都猜测一遍。实验表明其差分电流在2μA波动，没有明显的峰值，能够防御零值攻击，而没有采取防御方法的AES差分电流有明显峰值12μA。

2）对采用屏蔽方法的DES芯片提出改进的屏蔽方法。在数据进入S盒之前不恢复密钥，而是修改S盒，使得数据在经过S盒变换后能够消除屏蔽。DES算法中同时存在异或屏蔽和加法屏蔽，引入异或屏蔽和加法屏蔽之间相互安全转换的具体方法，使得算法中的敏感数据不以明文出现，能够完全屏蔽。功耗理论模拟攻击表明，其相关系数小于0.05，远远低于没有采用防御方法时的0.38，没有表现明显相关性，不能找出对应的密钥，能够防御关联攻击和重叠攻击。

3）针对DES加密系统的高阶DPA，研究表明UMM及几次改进方法不能防御，在其基础上提出算法层和逻辑层组合的防御方法。改进UMM算法；研究SABL逻辑特性，设计功耗平衡SABL逻辑单元库，半定制设计流程，并指出用SABL实现S盒的原因。本文实现基于SABL逻辑的功耗恒定标准单元库，对S盒的Spice网表进行模拟，得到一段电流特征曲线，其功耗曲线几乎相同，其特性与预期相吻合，与scCMOS相比，其功耗与输入信号的相关性大大降低。该算法的安全性分析和仿真实验表明可以防御高阶DPA攻击。

4）设计能够防御高阶DPA攻击的DES芯片。本文方法需2组额外的CMOS结构S盒以及用4组SABL结构S盒，1个随机数屏蔽。采用SABL实现DES芯片第1，2轮和第15，16轮，其功耗变化幅度几乎为0。用SABL逻辑实现DES不管UMM方法中第二轮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，它都可以防御功耗攻击。提高了这4轮防御选择明文及重叠攻击的能力，弥补UMM的薄弱环节，使Lv攻击方法失效。采用CMOS实现非关键部分模块，最后构成整体DES芯片。设计实现芯片时考虑智能卡的限制，在一些指标的选择上进行折中，采用部分流水结构实现智能卡，功耗和面积分别是全部采用SABL时的64.27%和66.67%。本文设计的芯片功耗与输入数据相关性降低，其NED值为2.32%。加密一次约耗时70ms。对其进行性能仿真分析，芯片能够实现加密/解密，能够防御高阶DPA攻击，比以前的方法节省资源。

由于DPA技术日趋成熟，其攻击力和危害性越来越大，特别是高阶DPA攻击的实施和应用，对现代加密芯片构成巨大威胁，芯片的安全性必须要考虑防御高阶DPA攻击。结合本文的工作，以及当前DPA攻击和高阶DPA攻击的最新研究成果，提出今后进一步的研究工作展望和设想：

1）现有文献提出很多针对SPA和DPA的防御方法，使得SPA和DPA攻击失效。高阶DPA攻击能力更强，同时其实施成本越来越低，因此研究高阶DPA攻击是一个新的趋势。与此相应的是如何对其实施高效低成本的防御，成为当前研究的热点和难点。

2）针对具体算法的各种改进型功耗攻击，其利用具体算法的特点，因此攻击能力更强，同样更加难以防御，AES和RSA就分别受到具有针对性的零值攻击和轨迹攻击。针对主流加密算法研究新的专用攻击方法，提高攻击效

率是一个新的研究重点，同时提出相应的防御方法也将是研究重点。主动研究新的攻击方法，才能够有针对性地提出防御方法。既要有能攻击对手芯片的更锋利的“矛”，也要有保护自己芯片的更坚固的“盾”。

功耗攻击和防御方法具有广阔的应用前景，对信息安全具有现实意义，需要解决的问题众多，还需要更多的研究人员投入到这一问题的研究中来。

参考文献

[1] 杨波. 现代密码学. 清华大学出版社. 2003 年

[2] Bruce Schneie 著，吴世忠等译. 应用密码学——协议、算法与 C 源程序. 机械工业出版社. 2000 年

[3] 刘连浩. 高级加密标准及短分组加密技术应用研究. 中南大学博士学位论文. 2006 年

[4] 丁群，彭喜元，杨自恒. 基于神经网络算法的组合序列密码芯片. 电子学报. 2006，34(3)：409-412 页

[5] Chen Z M and Zhou Y J. Dual-rail random switching logic: a countermeasure to reduce side channel leakage. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Yokohama, Japan, 2006:242-254P

[6] Biham E and Shamir A. Differential cryptanalysis of the data encryption sandard. New York: Springer-Verlag, 1993

[7] Biryukov A and Wagner D. Slide attacks. Proceedings of International Workshop on Fast Software Encryption, Rome, Italy, 1999:245-259P

[8] 张闻宇. 高级加密标准的研究. 山东大学博士学位论文. 2007 年

[9] Biham E. New types of cryptanalytic attacks using related keys. Proceedings of Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology, Lofthus, Norway, 1994:398-409P

[10] Biham E, Biryukov A and Shamir A. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. Journal of Cryptology, 2005, 18(4):291-311P

[11] Biham E, Dunkelman O and Keller N. The rectangle attack-rectangling the serpent. Proceedings of International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology, Innsbruck (Tyrol), Austria, Springer-Verlag, 2001:340-357P

[12] Paul N. Fahn, Peter K. Pearson. IPA: A new class of power attacks. Proceedings of Workshop on Cryptographic Hardware and Embedded

Systems, Worcester, Massachusetts, USA, 1999:173-186P

[13] Las R. Knudsen. Truncated and higher order differentials. Proceedings of International Workshop on Fast Software Encryption, Leuven, Belgium, 1994:196-211P

[14] David Wagner. The boomerang attack. Proceedings of International Workshop on Fast Software Encryption, Rome, Italy, 1999:156-170P

[15] Kocher P, Jaffe J and Jun B. Differential power analysis. Proceedings of International Cryptology Conference, Santa Barbara. California, USA, 1999:388-397P

[16] Oswald E. On side-channel attacks and the application of algorithmic countermeasures. [Thesis for PhD].Graz, Ausrtia:Graz University of Technolog,2003

[17] John Kelsey, Bruce Schneier, David Wagner, Chris Hall. Side channel cryptanalysis of product ciphers. Proceedings of European Symposium on Resarch in Computer Security, Toulouse, France, 1998:97-110P

[18] Muir J A. Techniques of side channel cryptanalysis. [Thesis for Master]. Waterloo，Ontario，Canada: University of Waterloo, 2001

[19] Hess E, Janssen N and Meyer B. Information leakage attacks against smart card implementations of cryptographic algorithms and countermeasures a survey. Proceedings of Eurosmart Security Conference. Sophia Antipolis, French, 2000:55-64P

[20] Peeters E, Standaert F X and Quisquater J J. Power and electromagnetic analysis: improved model, consequences and comparisons. Integration the VLSI Journal. 2007,40(1):52-60P

[21] Tiri K, Schaumont P and Verbauwhede I. Side-channel leakage tolerant architectures. Proceedings of International Conference on Information Technology, New Generations, Las Vegas, Nevada, 2006:204-209P

[22] Giorgetti J, Scotti G, Simonetti A and Trifiletti A. Analysis of data dependence of leakage current in CMOS cryptographic hardware. Proceedings of Great Lakes Symposium on VLSI, Stresa-Lago Maggiore,

Italy, 2007:78-83P

[23] Ors S B, Gurkaynak F, Oswald E and Preneel B. Power-analysis attack on an ASIC AES implementation. Proceedings of the International Conference on Information Technology: Coding and Computing, Las Vegas, USA, 2004:546-553P

[24] 童元满，王志英，戴葵，陆洪毅. 识别密码算法具体实现中潜在功耗攻击的理论分析方法. 计算机辅助设计与图形学学报. 2008，20(3)：395-402 页

[25] Okeya K and Iwata T. Side channel attack on message authentication codes. Proceedings of European Workshop on Security and Privacy in Ad hoc and Sensor Networks 2005:205-217P

[26] JaeCheol Ha, ChangKyun Kim, SangJae Moon, IlHwan Park, HyungSo Yoo. Differential power analysis on block cipher ARIA. Proceedings of High Performance Computing and Communcations, 2005:541-548P

[27] Kwon D, Kim J, Park S, Sung S H, Sohn Y, Song J H, Yeom Y, Yoon E, Lee S, Lee J, Chee S, Han D and Hong J. New block cipher: ARIA Proceedings of Information Security and Cryptology, 2004:432-445P

[28] Dakshi A, Josyula R, Pankaj R and Kai S. Templates as master keys. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Edinburgh UK, 2005:15-29P

[29] Tiri K and Verbauwhede I. Simulation models for side-channel information leaks. Proceedings of Design Automation Conference, Anaheim, California, USA, 2005:228-233P

[30] Suzuki D, Saeki M and Ichikawa T. DPA Leakage models for CMOS logic circuits. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Edinburgh UK,2005:366-382P

[31] Li H, Markettos A T and Moore S. Security evaluation against electromagnetic analysis at design time. Proceedings of High-Level Design Validation and Test Workshop, Napa Valley, California, USA, 2005:211-218P

[32] Karine G, Christophe M and Francis O. Electromagnetic analysis: concrete

results. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Paris, France, 2001:251-261P

[33] Josyula R R. Pankaj R.Empowering side channel attacks. Cryptology ePrint Archive. http://eprint.iacr.org/.IACR.037/2001

[34] Agrawal D, Archambeault B, Rao J R and Rohatgi P. The EM side-channel(s). Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Redwood Shores, California, USA, 2002:29-45P

[35] Dhem J F, Koeune F, Leroux P A, Mestre P, Quisquater J J and Willems J L. A practical implementation of the timing attack. Proceedings of International Conference on Smart Card Research and Applications, Louvain-la-Neuve, Belgium,1998:167-182P

[36] Biham E and Shamir A. Differential fault analysis of secret key cryptosystems. Proceedings of International Cryptology Conference on Advances in Cryptology. Santa Barbara. California,USA,1997:513-525P

[37] Skorobogatov S P and Anderson R J. Optical fault induction attacks. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Redwood Shores, California, USA, 2002:2-12P

[38] Piret G and Quisquater J J. A differential fault attack technique against SPN structures with application to the AES and KHAZAD. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Cologne, Germany, 2003:77-88P

[39] 李翔宇. 密码集成电路的非算法抗功耗分析设计方法研究. 清华大学博士学位论文. 2005 年

[40] Wang L Y. On the hardware design for DES cipher in tamper resistant devices against differential fault analysis. Proceedings of International Symposium on Circuits and Systems, Geneva, Switzerland, 2000:697-700P

[41] Agrawal D, Rao J R and Rohatgi P. Multi-channel attacks. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems.Cologne, Germany, 2003:2-16P

[42] Fournier J J A, Moore S, Li H, Mullins R and Taylor G. Security evaluation

of asynchronous circuits. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Cologne, Germany, 2003:137-151P

[43] Potlapally N R, Raghunathan A, Rav S, Jha N K and Lee R B. Satisfiability-based framework for enabling side-channel attacks on cryptographic software. Proceedings of the Design, Automation and Test in Europe Conference and Exhibition, Munich, Germany, 2006:18-23P

[44] Chandrakasan A P, Shen S and Brodersen R W. Low-power CMOS digital design. IEEE Journal of Solid-State Circuits, 1992, 27(4):473-484P

[45] 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)：1646-1652 页

[46] Tiri K, Akmal M and Verbauwhede I. A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards. Proceedings of European Solid-State Circuits Conference, Florence, Italy,2002:403-406P

[47] 李翔宇，孙义和. 用于密码芯片抗功耗攻击的功耗平衡加法器. 半导体学报. 2005，26(8)：1629-1634 页

[48] Lu X and Heys H M. A simple power analysis attack against the key schedule of the Camellia block cipher. Information Processing Letters. 2005, 95(3):409-412P

[49] Aoki K, Ichikawa T, Kanda M, Matsui M, Moriai S, Nakajima J and Tokita T. Camellia: a 128-bit block cipher suitable for multiple platforms-design and analysis. Proceedings of Symposium on Applied Computing. Villa Olmo, Como, Italy, 2000:39–56P

[50].Messerges T S, Dabbish E A and Slona R H. Investigations of power analysis attacks on smartcards. Proceedings of the USENIX Workshop on Smartcard Technology, Illinois, Chicgao, USA, 1999:151-161P

[51] Schindler W, Lemke K and Paar C. A stochastic model for differential side channel cryptanalysis. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Edinburgh, UK, 2005:30-46P

[52] Tiri K, Hwang D, Hodjat A, Lai B, Yang S, Schaumont P and Verbauwhede I.

A side-channel leakage free coprocessor IC in 0.18μm CMOS for embedded AES-based cryptographic and biometric processing. Proceedings of Design Automation Conference, Anaheim, California, USA, 2005:388-394P

[53] Messerges T S. Using second-order power analysis to attack DPA resistant software. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Worcester, Massachusetts, USA, 2000:238-251P

[54] Oswald E, Mangard S and Herbst C. Practical second-order DPA attacks for masked smart card implementations of block ciphers. Proceedings of The Cryptographers' Track at the RSA Conference, San Jose, California, USA, 2006:192-207P

[55] 蒋惠萍，毛志刚. 一种抗差分功耗攻击的改进 DES 算法及其硬件实现. 计算机学报. 2004，27(3)：334-338 页

[56] Joye M, Paillier P and Schoenmakers B. On second-order differential power analysis. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Edinburgh, UK, 2005:293-308P

[57] Waddle J and Wagner D. Towards efficient second-order power analysis. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Cambridge, Massachusetts, USA, 2004:1-15P

[58] Peeters E, Standaert F X, Donckers N and Quisquater J J. Improved higher-order side-channel attacks with FPGA experiments. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Edinburgh UK ,2005:309-323P

[59] Brier E, Clavier C and Olivier F. Correlation power analysis with a leakage model. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Cambridge, Massachusetts, USA, 2004:16–29P

[60] Akkar M L and Goubin L. A generic protection against high-order differential power analysis. Proceedings of International Workshop on Fast Software Encryption, Lund, Sweden, 2003:192-205P

[61] 韩军，曾晓洋，汤庭鳌. RSA 密码算法的功耗轨迹分析及其防御措施. 计算机学报. 2006，29(4)：590-596 页

[62] Messerges T S,Dabbish E A and Sloan R H. Power analysis attacks of modular exponentiation in smartcards. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Worcester, Massachusetts, USA ,1999:144-157P

[63] Yen S M, Wei C L, Sang J M and Jaecheol H A. Power analysis by exploiting chosen message and internal collisions: vulnerability of checking mechanism for RSA-decryption. Proceedings of Progress in cryptology-Mycrypt2005, Kuala Lumpur, Malaysia, 2005:183-195P

[64] Regazzoni F, Badel S, Eisenbarth T, Großschadl J, Poschmann A, Toprak Z, Macchetti M, Pozzi L, Paar C, Leblebic Y i and Ienne P. A simulation-based methodology for evaluating the DPA-resistance of cryptographic functional units with application to CMOS and MCML technologies. Proceedings of International Symposium on Systems, Architectures, Modeling and Simulation, Samos, Greece, 2007:209-214P

[65] Rakers P, Connell L, Collins T and Russell D. Secure contactless smart card ASIC with DPA protection. IEEE Journal of Solid-State Circuits. 2001, 36(3):559-565P

[66] Shamir A. Protecting smart cards from passive power analysis with detached power supplies. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Worcester, Massachusetts, USA, 2000:71-77P

[67] Kocher P. Design and validation strategies for obtaining assurance in countermeasures to power analysis and related attacks. Proceedings of the NIST Physical Security Workshop, 2005:1-11P

[68] Muresan R, Vahedi H, Zhanrong Y and Gregori S. Power-smart system-on-chip architecture for embedded cryptosystems. Proceedings of International Conference on Hardware/Software Codesign and System Synthesis, Jersey City, New Jersey, 2005:184-189P

[69] Bucci M, Luzzi R, Guglielmo M and Trifiletti A. A countermeasure against differential power analysis based on random delay insertion. International Symposium on Circuits and Systems, 2005:3547-3550P

[70] Yang S, Wolf W, Vijaykrishnan N, Scrpanos D N and Xie Y. Power attack resistant cryptosystem design: a dynamic voltage and frequency wwitching approach. Proceedings of the Design, Automation and Test in Europe Conference and Exhibition, Munich, Germany, 2005:64-69P

[71] Daemen J, Peeters M and Assche G V. Bitslice ciphers and power analysis attacks. Proceedings of International Workshop on Fast Software Encryption, New York, USA, 2000:134-149P

[72] Golic J D and Tymen C. Multiplicative masking and power analysis of AES. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Redwood Shores, California, USA, 2003:31-47P

[73] Goubin L and Patarin J. DES and differential power analysis-the duplication method. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Worcester, Massachusetts, USA, 1999:158-172P

[74] Chari S, Jutla C, Rao J R and Rohatgi P. A cautionary note regarding evaluation of aes candidates on smart-cards. Proceedings of the Second Advanced Encryption Standard Candidate, Yorktown Heights, NY, USA, 1999:1-15P

[75] Trichina E, Seta D D and Germani L. Simplified adaptive multiplicative masking for AES. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, RedwoodShores, California, USA, 2002:187-197P

[76] Chari S, Jutla C S, Rao J and Rohatgi P. Towards sound approaches to counteract power-analysis attacks. International Cryptology Conference on Advances in Cryptology, Santa Barbara, California, USA, 1999:398-412P

[77] Courtois N T and Goubin L. An algebraic masking method to protect AES against power attacks. Proceedings of Information Security and Cryptology, Beijing, China, 2005:199-209P

[78] Trichina E and Korkishko T. Secure AES hardware module for resource constrained devices. Proceeding of Security in Ad-hoc and Sensor Networks, Heidelberg, Germany, 2004:215-229P

[79] Trichina E and Korkishko L. Secure and efficient AES software

implementation for smart cards. Proceeding of Information Security Applications, Jeju Island, Korea, 2004:425-439P

[80] Akkar M L and Giraud C. An implementation of DES and AES, secure against some attacks. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Paris, France, 2001:309-318P

[81] Blomer J, Guajardo J and Krummel V. Provably secure masking of AES. Proceeding of Selected Areas in Cryptography, Waterloo, Ontario, Canada, 2004: 69-83P

[82] Oswald E, Mangard S, Pramstaller N and Rijmen V. A side-channel analysis resistant description of the AES S-Box. Proceedings of International Workshop on Fast Software Encryption, Paris, France, 2005:413-423P

[83] Zhang N, Chen Z and Xiao G. Efficient elliptic curve scalar multiplication algorithms resistant to power analysis. Information Sciences, 2007, 177(10):2119-2129P

[84] Catherine H and Gebotys S. A table masking countermeasure for low-energy secure embedded systems. IEEE Transactions on VLSI Systems, 2006,14(7):740-753P

[85] Fouque P A, Muller F, Poupard G and Valette F. Defeating countermeasures based on randomized BSD representations. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Cambridge, Massachusetts USA, 2004:312-327P

[86] Hasan M A. Power analysis attacks and algorithmic approaches to their countermeasures for Koblitz curve cryptosystems.IEEE Transactions on computers, 2001, 50(10):1071-1083P

[87] Dupuy W and Sebastien K J. Resistance of randomized projective coordinates against power analysis, Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Edinburgh, UK, 2005:1-14P

[88] Lv J and Han Y. Enhanced DES implementation secure against high-order differential power analysis in smartcards. Proceedings of Australasian

Conference on Information Security and Privacy, Townsville, Queensland, Australia, 2005:195-206P

[89] Park J H, Lee H J, Ha J C, Choi Y, Kim H W and Moon S J. A differential power analysis attack of block cipher based on the hamming weight of internal operation unit. International Conference on Computational Intelliquence and Security, Guangzhou, China, 2006:1375-1380P

[90] Handschuh H and Prenee B. Blind differential cryptanalysis for enhanced power attack. Proceedings of Selected Areas in Cryptography, Montreal, Quebec, Canada, 2006:163-173P

[91] 陈志敏. 安全芯片旁路功耗分析及抗攻击措施. 上海交通大学硕士学位论文. 2007 年

[92] Moore S, Anderson R, Cunningham P, Mullins R and Taylor G. Improving smart card security using self-timed circuits. International Symposium on Asynchronous Circuits and Systems, Manchester, UK, 2002:211-218P

[93] Tiri K and Verbauwhede I. Charge recycling sense amplifier based logic: securing low power security IC's against DPA. European Solid-State Circuits Conference, Leuven, Belgium, 2004:179-182P

[94] Tiri K and Verbauwhede I. A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation. Proceedings of the Design, Automation and Test in Europe Conference and Exhibition, Paris, France, 2004:246-251P

[95] Tiri K and Verbauwhede I. A VLSI design flow for secure side-channel attack resistant ICs. Proceedings of the Design, Automation and Test in Europe Conference and Exhibition, Munich, Germany, 2005:58-63P

[96] 童元满，王志英，戴葵，陆洪毅，石伟. 基于 WDDL 和行波流水技术的抗功耗攻击高性能分组密码协处理器设计与实现. 计算机学报. 2008，31(5)：827-834 页

[97] Sokolov D, Murphy J, Bystrov A and Yakovlev A. Improving the security of dual-rail circuits. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems. Boston Marriott Cambridge Cambridge, Massachusetts,

USA, 2004:282-297P

[98] Popp T and Mangard S. Implementation aspects of the DPA-resistant logic style MDPL. International Symposium on Circuits and Systems, Island of Kos, Greece, 2006:2913-2916P

[99] Ilham H, Francois M, Denis F and Legat J D. Low-swing current mode logic: A new logic style for secure and robust smart cards against power analysis attacks. Microelectronice Journal, 37(9), 2006:997-1006P

[100] 童元满，王志英，戴葵，石伟，陆洪毅. 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)：935-939 页

[101] Golic J D. Techniques for random masking in hardware. IEEE Transactions on Circuits and Systems, 2007, 54(2):291-300P

[102] Mace F, Standaert F X, Quisquater J J and Legat J D. A design methodology for secured ICs using dynamic current mode logic. Power and Timing Modeling, Optimization and Simulation, Leuven, Belgium, 2005:550-560P

[103].Gurkaynak F K, Oetiker S, Kaeslin H, Felber N and Fichtner W. Design challenges for a differential-power-analysis aware GALS-based AES crypto ASIC. Electronic Notes in Theoretical Computer Science, 2005, 146:133-149P

[104] Gurkaynak F, Oetiker S, Kaeslin H, Felber N and Fichtner W. Improving DPA security by using Globally-Asynchronous Locally-Synchronous systems. Proceedings of the European Solid-State Circuits, Grenoble, France, 2005:407-410P

[105] Mangard S, Popp T and Gammel B M. Side-channel leakage of masked CMOS gates. Proceedings of the RSA Conference Cryptographers' Track., San Francisco, USA, 2005:351-365P

[106] Mangard S, Pramstaller N and Oswald E. Successfully attacking masked AES hardware implementations. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Edinburgh, UK, 2005:157-171P

[107] Akkar M L, Bevan R and Goubin L. Two power analysis attacks against one-mask methods. International Workshop on Fast Software Encryption, Delhi, India, 2004:332–347P

[108] 赵佳，曾晓洋，韩军，陈俊. 简化的抗零值功耗分析的 AES 算法及其 VLSI 实现. 计算机工程. 2007，33(16)：220-222 页

[109] 赵佳，曾晓洋，韩军，王晶，陈俊. 抗差分功耗分析攻击的 AES 算法的 VLSI 实现. 计算机研究与发展. 2007，44(3)：378-383 页

[110] 陈毅成，邹雪城，刘政林，韩煜. 针对高级数据加密标准的最大差分功耗分析. 华中科技大学学报(自然科学版). 2007，35(11)：96-98 页

[111] Oswald E and Schramm K. An efficient masking scheme for AES software implementations. Workshop on Information Security Applications, Jeju Island, Korea, 2005:292-305P

[112] Herbst C, Oswald E, and Mangard S. An AES smart card implementation resistant to power analysis attacks. Applied Cryptography and Network Security, Singapore, 2006:239-252P

[113] Guilley S, Hoogvorst P and Pacalet R. Differential power analysis model and some results. Proceedings of Smart Card Research and Advanced Application Conference, Toulouse, France, 2004:127-142P

[114] 孙骏，韩泽耀. 一种抗 DPA 攻击的 DES 设计. 中国集成电路. 2006，5：28-31 页

[115] Messerges T S. Securing the AES finalists against power analysis attacks. International Workshop on Fast Software Encryption, New York, NY, USA, 2000:150-164P

[116] 蒋惠萍，毛志刚. 防止差分功耗分析的安全 DES 模块的 MASK 技术研究. 电子器件. 2003，26(2)：169-172 页

[117] Coron J S and Goubin L. On boolean and arithmetic masking against differential power analysis. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Worcester, Massachusetts, USA, 2000:231-237P

[118] Goubin L. A sound method for switching between boolean and arithmetic

masking. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Paris, France, 2001:3-15P

[119] Lv J. On two DES Implementations secure against differential power analysis in smart-cards. Information and Computation, 2006, 204(7):1179-1193P

[120] Tiri K and Verbauwhede I. Design method for constant power consumption of differential logic circuits. Proceedings of the Design, Automation and Test in Europe Conference and Exhibition, Munich, Germany, 2005:628-633P

[121] 石伟，戴葵，童元满，龚锐，王志英. 防 DPA 攻击的两种不同逻辑比较研究. 计算机工程与科学. 2007，29(5)：19-22 页

[122] 石伟，戴葵，童元满，龚锐. 防 DPA 攻击的标准单元库的设计与实现. 微电子学与计算机. 2007，24(2)：51-54 页

[123] Tiri K and Verbauwhede I. A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation. Proceedings of the Design, Automation and Test in Europe Conference and Exhibition, Paris, France, 2004:246-251P

[124] Wong K, Wark M and Dawson E. A single-chip FPGA implementation of the Data Encryption Standard(DES) algorithm. IEEE Global Telecommunications Conference, Sydney, Australia,1998:827-832P

[125] 蒋惠萍. 抗功耗分析的加密算法硬件设计技术研究. 哈尔滨工业大学博士学位论文. 2005 年

[126] Messerges T S, Dabbish E A and Sloan R H. Examining smart-card security under the threat of Power analysis attacks. IEEE Transactions on Computers, 2002, 51(5):541-552P

攻读博士学位期间发表的论文和取得的科研成果

[1] 李海军，马光胜，冯刚，刘艳葆，孙强. 一种抗差分功耗分析 DES 的算法. 哈尔滨工业大学学报，2006 年 7 月，38 卷(增刊)：660-662P

[2] Li Haijun, Zhou Tao, Ma Guangsheng, Liu Yaobao, Lu Huiling. Algorithm against differential power analysis base on sequence code mask. Journal of Harbin Institute of Technology, 2007, 14(SUP):193-195P (EI:072210627338)

[3] Li Haijun, Ma Guangsheng, Li Guangshun, Wang Guanjun, Zhou Tao. A new protect cryptographic circuit approach using dynamic current model logic circuit. Proceedings of International Conference on Mechatronics and Automation, Harbin, China, 2007:2221-2225P (EI: 075110979574)

[4] Li Haijun, Zhou Tao, Lu Huiling, Liu Xiaoxiao. A new methodology protect smart cards from DPA. Proceedings of International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, Hangzhou, China, 2007:1383-1386P (EI: 083011402847)

[5] Li Haijun, Zhou Tao, Lu Huiling, Sun Qiang. Using complement register structure circuit against H-O DPA. Proceedings of International Conference on Innovative Computing, Information and Control, Kumamoto, Japan, 2007:599-603P (EI: 080811103192)

[6] Li Haijun, Zhou Tao, Lu Huiling, Sun Qiang. A new method against high-order differential power analysis. Proceedings of International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, China, 2007:3047-3050P (EI: 080311027698)

[7] 李海军，马光胜，刘晓晓. DES 芯片抵御高阶差分功耗分析攻击方法研究. 半导体学报. 2008，29(2)：376-380P (EI: 081311170539)

致　谢

博士研究生的学习阶段即将结束，期间的学习和研究生活既紧张又充实，使我学到了许多新知识，锻炼、培养了自己分析、解决问题的能力。在这里，我要首先感谢导师马光胜教授，感谢他多年来对我多方面的关怀和启迪。本论文各阶段的设计、论证和实现，都得到了马老师的精心指导和帮助。他严谨的治学态度、敏锐的学术眼光、渊博的学识使我受益非浅。在此对马老师致以深深的谢意。

感谢实验室的冯刚博士、李东海、李光顺、朱学仕、吴俊华、王秀芹、胡靖、王冠军、孙强、刘晓晓、邵晶波、宋朝晖、金英，与他们朝夕相处，结下了深厚的友谊。和他们的讨论交流过程中，我开阔了视野，增长了知识。

在此，谨以此文向关心和帮助过我的所有老师、同学、朋友和家人表示我最衷心的感谢！

加密芯片的旁道攻击防御对策研究

作者：李海军
学位授予单位：哈尔滨工程大学