防御差分功耗分析攻击技术研究

汪鹏君* 张跃军 张学龙
(宁波大学电路与系统研究所 宁波 315211)

摘 要：差分功耗分析(DPA)攻击依赖于密码芯片在执行加密/解密过程中功耗与数据及指令的相关性，利用统计学等方法对收集到的功耗曲线进行分析，盗取关键信息，对密码芯片的安全性构成极大威胁。防御 DPA 攻击技术的开发与研究，已经成为信息安全领域的迫切需求。该文在归纳 DPA 攻击原理的基础上，对主流防御 DPA 攻击技术的理论与设计方法进行概述与分析，指出防御 DPA 前沿技术的研究进展。重点讨论防御 DPA 攻击技术的原理、算法流程和电路实现，包括随机掩码技术、功耗隐藏技术、功耗扰乱技术等等，并详细分析这些技术存在的优缺点。最后，对该领域潜在的研究方向与研究热点进行探讨。

关键词：信息安全；密码芯片；差分功耗分析(DPA)攻击；防御技术
中图分类号：TP309 **文献标识码**： A **文章编号**：1009-5896(2012)11-2774-11
DOI: 10.3724/SP.J.1146.2012.00555

Research of Differential Power Analysis Countermeasures

Wang Peng-jun Zhang Yue-jun Zhang Xue-long
(*Institute of Circuits and Systems*, *Ningbo University*, *Ningbo* 315211, *China*)

Abstract: Differential Power Analysis (DPA) attacks exploit the data or instruction dependency of the power consumption of the cryptographic devices during encryption/decryption process. A large number of power traces are used to analyze the cipher key information on mathematics statistical methods. DPA attacks have been becoming a great threat to cipher security. In order to systematically and comprehensively understand DPA countermeasures, and actively promote the studying of high performance cryptographic chip, this paper introduces the basic principle of DPA, explains and analyzes the mainstream DPA countermeasures, and points out the advanced topics countermeasures. This paper focuses on the theory of DPA countermeasures, the flow path of algorithm, and the implementation of circuits, including masking technology, hiding technology, power disruption technology and so on. The advantages and disadvantages of these countermeasures are detailed discussed. Finally, the potential research directions and advanced topics on DPA countermeasures are provided.

Key words: Information security; Cryptography; Differential Power Analysis (DPA); Countermeasures

1 引言

随着超大规模集成电路(Very Large Scale Integration, VLSI)和计算机技术的发展，信息安全已从传统的政治、军事、外交、情报等重要领域全面推广到社会日常生活中。由于信息安全技术确保了各种关键信息的安全保存和传输，因此高性能智能卡在我国已经非常普及，如银行卡、身份证、交通卡、手机卡等，为人们生活带来了便利。现代电子设备由集成电路构成，信息安全技术也依赖于相应的集成电路(如密码芯片)作为硬件载体。密码芯片是信息安全的保障，它有效地实现用户的身份验证、密钥存储等关键信息的保护。随着集成电路各种性能要求的提高，其单片集成度按摩尔规律不断增长，高性能密码芯片的 VLSI 设计技术已经成为信息化社会的迫切需求。信息安全的攻击和防御始终是一对“矛”和“盾”，一方为了推广智能卡的使用，必须确保信息的安全，有效防御外界的攻击，筑起坚固的“盾”以防信息的泄漏，可称之为信息安全的“防御”；而另一方则不择手段，磨砺锋利的“矛”以攻克对方的“盾”，盗取其重要信息，可称之为信息安全的“攻击”，就好像计算机病毒软件和杀病毒软件一样，这对“矛盾”在不断进化、升级。因此对信息安全的攻击和防御方法的研究越来越受到学者们的关注。

传统攻击使用数学分析的方法寻找加密算法的

2012-05-11 收到，2012-09-03 改回
国家自然科学基金(61274132, 61076032)，教育部博士点基金(20113305110005)和优秀博士学位论文培育基金(PY20100003)资助课题
*通信作者：汪鹏君 wangpengjun@nbu.edu.cn

漏洞，要求攻击者必须在密码分析和加密算法方面有相当高的造诣，而新型攻击技术除此之外还可通过其他途径盗取信息。众所周知，目前普遍采用将保密信息通过在加密器件上执行密码算法的策略，达到保护信息安全的目的，然而，在执行密码算法过程中物理器件总是要泄漏各种与密码系统本身相关的信息，譬如运行时间、能量消耗、电磁辐射等等。攻击者利用这些边际信息攻击加密器件就可获得密钥，这一过程称为旁道攻击[1](Side Channel Attack, SCA)。旁道攻击方法分为时间分析[2]、功耗分析[3]和电磁辐射分析[4]3 类。在旁道信息中，由于功耗的可测试性最强、测试功耗的工具最简单、功耗曲线也最适合分析，使得功耗分析攻击在实际攻击中应用最多。功耗分析就是依赖于加密硬件在加密过程中电路功耗与其处理的数据及进行的操作关联，通过监测硬件在加密过程中的功耗曲线，利用统计方法和攻击者的经验对收集到的信息进行分析，从而获得与加密信息相关的数据。在诸多功耗分析旁道攻击方案中，差分功耗分析[3](Differential Power Analysis, DPA)攻击技术被证明是最有效率并且是最容易实现的一种，由于其易于操作且非常有效，对密码模块的安全构成重大威胁。

国际发卡组织 VISA 非常重视 DPA 攻击对密码芯片的危害，以至于该组织将芯片信用卡的安全需求提升为 3 个技术等级，而在安全性级别最高的技术等级中明确提出至少包含 1 个以上对策来防止 DPA 等信息泄露攻击技术，可见 DPA 攻击具有极大的杀伤力。防止 DPA 攻击对实际应用中的加密器件安全性造成威胁，开发具有防御 DPA 攻击的 VLSI 密码芯片，具有重大理论价值和现实意义。

2　DPA 攻击的基本原理

DPA 攻击是 Kocher 等人[3]于 1999 年提出来的，它是一门结合了统计分析与误差修正的技术，利用不同明文输入对应不同功耗曲线，推断密码算法中与密钥相关的部分信息。对于密码系统来说，功耗的变化主要由内部寄存器状态跳变引起，统计学上表现为内部数据的汉明距离(Hamming Distance, HD)或汉明重量(Hamming Weight, HW)。简单来说，DPA 成功的基础是大量的功耗曲线样本，再结合相关统计学方面的知识，其基本流程包括功耗样本采集，理论功耗模型建立，密钥猜测，功耗偏差分析和密钥判断[5,6]等，如图 1 所示。

首先 DPA 攻击者随机选择 n 个明文作为输入进行 N 次加密运算，对应于每一次的加密运算的明文 P_i，搜集相应的离散功耗信号 S_{ij}，以及相应的输出

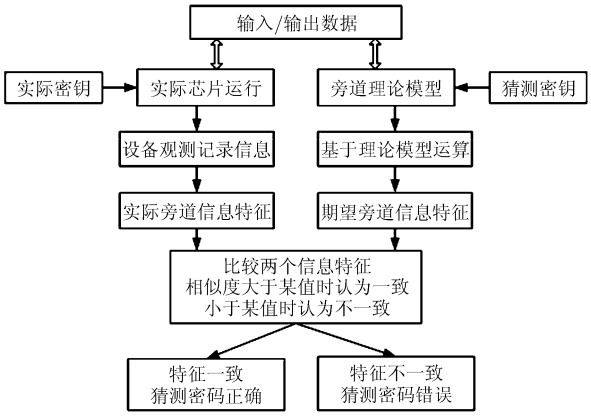


图 1 DPA 攻击的基本流程

密文 O_i。功耗信号 S 中的 i 和明文输入 P 中的 i 相关，j 和采样时间相关。则可使用选择函数 $D(\cdot,\cdot,\cdot)$ 把 S_i 分成两部分：

$$S_0 = \{S_{ij} \mid D(\cdot,\cdot,\cdot) = 0\} \tag{1}$$

$$S_1 = \{S_{ij} \mid D(\cdot,\cdot,\cdot) = 1\} \tag{2}$$

然后计算每一部分的平均功耗为

$$A_0[j] = \frac{1}{|S_0|}\sum_{S_{ij}\in S_0} S_{ij} \tag{3}$$

$$A_1[j] = \frac{1}{|S_1|}\sum_{S_{ij}\in S_1} S_{ij} \tag{4}$$

其中 $|S_0|+|S_1| = N$。接下来计算离散的 DPA 偏差信号 $T[j]$。

$$T[j] = A_0[j] - A_1[j] \tag{5}$$

如果运算中涉及了选择函数的某位或包含这个位的数据时，该数据的值是 0 或 1 会对功耗曲线的幅值有细小的影响。假定这个细小的差别为 ε，并且在时间 j^*时计算 D 函数，则功耗之间的数学期望 E 可用下式表示：当 $j = j^*$时，加密模块执行密钥比特，则功耗大小与 D 函数相关

$$\varepsilon = E[S_{ij} \mid D(\cdot,\cdot,\cdot) = 0] - E[S_{ij} \mid D(\cdot,\cdot,\cdot) = 1] \neq 0 \tag{6}$$

当 $j \neq j^*$时，加密模块执行其他比特，则功耗大小与 D 函数无关

$$\begin{aligned}\varepsilon &= E[S_{ij} \mid D(\cdot,\cdot,\cdot) = 0] - E[S_{ij} \mid D(\cdot,\cdot,\cdot) = 1] \\ &= E[S_{ij}] - E[S_{ij}] = 0\end{aligned} \tag{7}$$

从式(6)和式(7)可知，如果采样明文足够多，则 $T[j]$ 就能计算出在时间 j 时的功耗差分 ε。为了更好地探讨防御 DPA 攻击的方法，文献[1]将式(6)改写为

$$r = \frac{\sum_{i=1}^{n}(x_i - \overline{x})\cdot(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \overline{x})^2 \cdot \sum_{i=1}^{n}(y_i - \overline{y})^2}} \tag{8}$$

其中 r 为功耗偏差值，x_i 为 i 时刻 0 值的功耗值，y_i 为 i 时刻 1 值的功耗值，$\overline{x}$ 为 x_i 的平均功耗，$\overline{y}$ 为 y_i 的平均功耗。从上述分析中可以知道，防御 DPA 攻击的主要思想就是使 r 尽可能地小，使之近似为 0。

3 主流防御 DPA 攻击技术的概述与分析

近年来，防御 DPA 攻击技术作为一个热点研究方向，在各个领域都引起了广泛关注，涉及 DPA 攻击的模型[7−9]、防御应用领域[10−14]和新的防御技术[15−19]等等。从 IEEE 历年文献的统计中可以发现，关于防御 DPA 攻击技术的研究呈逐年递增的态势，其主要途径大致可分为两类：一是尽量降低功耗曲线的波动，减小功耗曲线中的信息含量，即采用降低信噪比的方法达到防御 DPA 攻击的目的；二是尽量扰乱功耗曲线与数据的相关性，即采用增加随机噪声和冗余功耗达到防御 DPA 攻击的目的。这两种途径都可以提高密码芯片的安全性，使攻击者难以实施 DPA 攻击或者需要更多的功耗曲线样本。主流防御技术包括随机掩码技术[20−36]、功耗隐藏技术[37−51]和功耗扰乱技术[52−54]等等。

3.1 随机掩码技术

Kocher 等[3]在 1999 年首次提出使用随机掩码(Mask)技术来防御 DPA 攻击。Mask 技术利用攻击者不可能获取的随机变量 m 对密码算法的中间变量 V 进行掩盖，从而得到掩盖后的中间变量 $V_m(V_m = V \bullet m)$，使攻击者每次获取的功耗信息均由中间变量 V_m 产生，而且由于 m 是随机变化的，每次加密并不相同，所以攻击者将无法获得中间变量 V 所带来的功耗与密钥的相关性。由于加密过程中的各个操作均是与数据相关的，所以要求整个加密过程中所有的中间变量都被 m 所屏蔽。典型的 Mask 分为两种[6]：布尔型的 Mask，一般用异或操作实现 $x' = x \oplus r$；算术型的 Mask，一般用模加模乘来实现 $x' = (x - r) \bmod 2^k$。其中，布尔掩码与算术掩码可以相互转换，伪代码如表 1 所示。

表 1 伪代码

输入：布尔型掩码 $x = x' \oplus r$
输出：布尔型掩码的算术实现方式 $x = A \oplus r$
随机选择 $C = 0$ 或者 $C = -1$
$B = C \oplus r$; / $\cdot$ $B = r$ 或 $B = \overline{r} \cdot$ /
$A = B \oplus x'$; / $\cdot$ $A = x$ 或 $A = \overline{x} \cdot$ /
$A = A - B$; / $\cdot$ $A = x - r$ 或 $A = \overline{x} - \overline{r} \cdot$ /
$A = A + C$; / $\cdot$ $A = x - r$ 或 $A = \overline{x} - \overline{r} - 1 \cdot$ /
$A = A \oplus C$; / $\cdot$ $A = x - r \cdot$ /
Return(A, r).

在密码芯片 ASIC 实现时，将标准 CMOS 逻辑单元替换成具有防御 DPA 攻击特性的逻辑单元，就可以达到防御 DPA 攻击的目的[1]。而当前基于标准单元的 ASIC 设计中采用的标准库文件由集成电路制造厂商提供，采用静态互补 CMOS 逻辑实现，没有成熟的防御 DPA 攻击标准库文件。防御 DPA 攻击的标准单元库采用全定制流程实现：电路结构设计→功能验证→全定制版图设计→DRC/LVS/参数提取→后仿→标准库文件生成。基于 Mask 的标准单元如图 2 所示，其中 a 和 b 为输入信号，q 为输出信号；a_m 和 b_m 为 Mask 单元的输入信号，m_a 和 m_b 为对应的掩码，q_m 和 m_q 为掩码后输出信号；$\overline{a}_m$，$\overline{b}_m$，$\overline{m}$，$\overline{q}_m$ 为对应的互补信号。

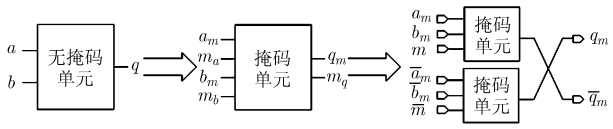


图 2 基于 Mask 的标准单元

在随机掩码算法与芯片实现方面，Yoshikawa 等人[20]提出多轮 Masking 方法防御 DPA 攻击和高效的随机数掩码方法[21]；Zhang 等人[22]提出一种能防御 DPA 攻击的椭圆曲线密码算法；Prouff 等人[23]提出利用置换表的方法防御一阶旁道攻击；Rivain 等人[30]提出将高阶 Mask[31−33]应用到高级加密标准(AES)算法中，实现防御 DPA 攻击。Mangard 等人[1]提出一种通用的掩码方法，将随机掩码用于 AES 密码算法，实现对电路中所有处理单元的输入和输出全部屏蔽，达到防御 DPA 攻击的目的。随机掩码 AES 加密算法包括掩码操作，轮密钥加，字节替换，行移位和列混淆等，如图 3 所示。其中，m_i' 为处理单元的输入输出状态，m 为屏蔽因子，字节替换中的非线性操作采用掩码后 Sbox 实现。

3.2 功耗平衡技术

功耗平衡技术可以从根本上解决功耗泄露密钥信息的问题，是近年防御 DPA 攻击的首选技术[37−51]。功耗平衡技术对密码芯片内部的存储信号采用汉明扩展编码进行重新编码，如比特“0”用“01”表示，而比特“1”用“10”表示。这就可以实现，从比特 0 变化到比特 1 和从比特 1 变化到比特 0 的状态变化都相同，因此也就难以区分汉明重量和比特翻转引起的功耗变化。从功耗分析上看，这个方法在理论上相对而言比较完善。但是从硬件实现上，它的资源消耗比较大，面积至少增加一倍以上，另外硬件实现上需要全部重新设计，没有相应的自动

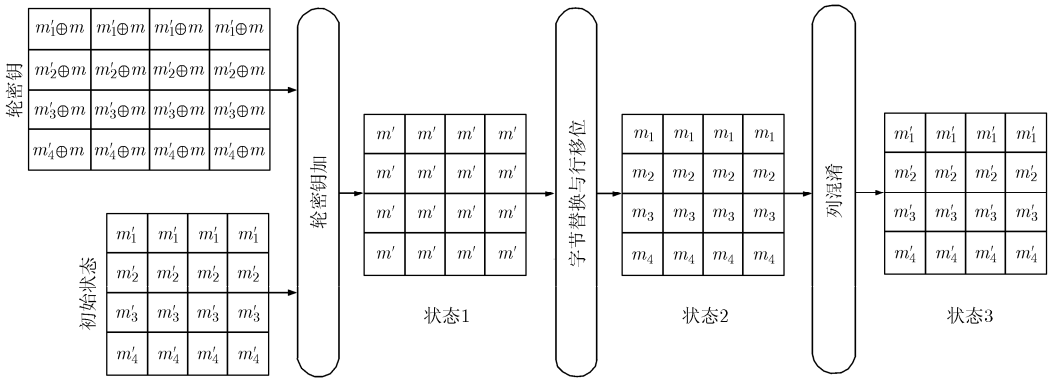


图 3 基于 Mask 的 AES 加密算法

化设计工具支持，比较费时费力。功耗隐藏技术研究已经非常成熟，相关功耗平衡逻辑电路也很多，主要包括双轨逻辑[37−43]、SABL 逻辑[40]、WDDL 逻辑[41]、MDPL 逻辑[42]和 DDSLL 逻辑[46]等等。

在静态互补 CMOS 逻辑中，只有输出发生 0→1 跳变时，逻辑门才消耗能量。双轨逻辑在一定程度上打破了数据与功耗的相关性，双轨逻辑结构模型如图 4 所示。C_{q0} 为输入端电容，C_{qw} 为线电容，C_{qj} 为输出端电容。

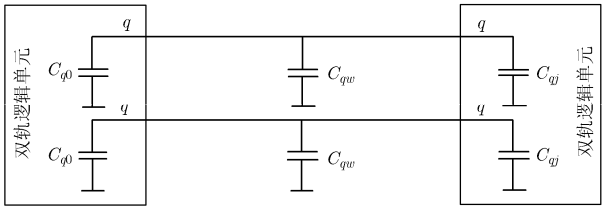


图 4 双轨逻辑结构模型

SABL 逻辑是双轨逻辑的一种实现方式，由于其预充电阶段的存在，当相邻时钟周期逻辑门输出状态相同时，逻辑门同样消耗能量。SABL 逻辑的功耗情况如表 2 所示。In_i 为第一轨当前输入，In_{i+1} 为第一轨次态输入，Out_i 为第一轨当前输出，Out_{i+1} 为第一轨次态输出；$\overline{\mathrm{In}}_i$ 为第二轨当前输入，$\overline{\mathrm{In}}_{i+1}$ 为第二轨次态输入，$\overline{\mathrm{Out}}_i$ 为第二轨当前输出，$\overline{\mathrm{Out}}_{i+1}$ 为第二轨次态输出。从表中可以看出，SABL 逻辑门输出信号的 4 种跳变(0→0, 0→1, 1→0, 1→1)消耗能量几乎相等，功耗大小不能反映逻辑门的实际输出状态，因此 SABL 逻辑门能够很好地防御 DPA 攻击。

WDDL 逻辑属于动态差分逻辑(Dynamic Differential Logic, DDL)类型，其中的门单元和触发器可以直接使用现有的 CMOS 标准单元库中的单元组合而成，不需要重新设计单元库。首先，以 WDDL 逻辑的二输入与门为例，其实现方法如图 5

表 2 SABL 逻辑的功耗

In_i→In_{i+1}	$\overline{\mathrm{In}}_i$ → $\overline{\mathrm{In}}_{i+1}$	Out_i→预充→Out_{i+1}	$\overline{\mathrm{Out}}_i$ →预充→ $\overline{\mathrm{Out}}_{i+1}$	消耗能量情况
0→0	1→1	0→1→0(有)	1→1→1(无)	消耗能量
0→1	1→0	0→1→1(有)	1→1→0(无)	消耗能量
1→0	0→1	1→1→0(无)	0→1→1(有)	消耗能量
1→1	0→0	1→1→1(无)	0→1→0(有)	消耗能量

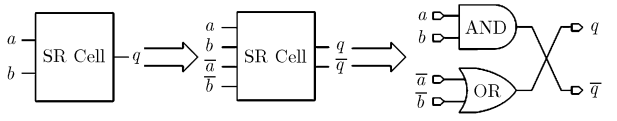


图 5 基于 WDDL 的与门

所示，其中 a 和 b 为输入信号，q 为输出信号；$\bar{a}$，$\bar{b}$，$\bar{q}$ 为对应的互补信号。WDDL 逻辑在 SDDL 逻辑的基础上进行扩展，由于 SDDL 逻辑门的一对输出信号在预充电阶段全为“0”，而在求值阶段结束后为互补信号，因此这两对信号可以直接作为下一级 SDDL 的输入，而不再需要预充电信号来进行控制，这样级联起来的逻辑即为 WDDL 逻辑[1]。

文献[41]在 0.18 μm CMOS 工艺下实现基于 AES 密码算法的嵌入式安全协处理器芯片，如图 6 所示。该芯片可应用在指纹识别上，包括密码算法模块，指纹匹配模块，模板存储单元以及接口电路等。该芯片由两个处理器构成，32 bit SPARC V8 处理器使用标准 CMOS 库实现，第 2 个协处理器使用 WDDL 逻辑实现。该嵌入式安全协处理器芯片采用两种方式防御 DPA 攻击：第 1 种方法为 WDDL 逻辑，使所有逻辑门在每个时钟周期都消耗相同的功耗；第 2 种方法称为口令路由识别，确保 WDDL 逻辑在输出节点上 0 和 1 的数量完全相同。对该安

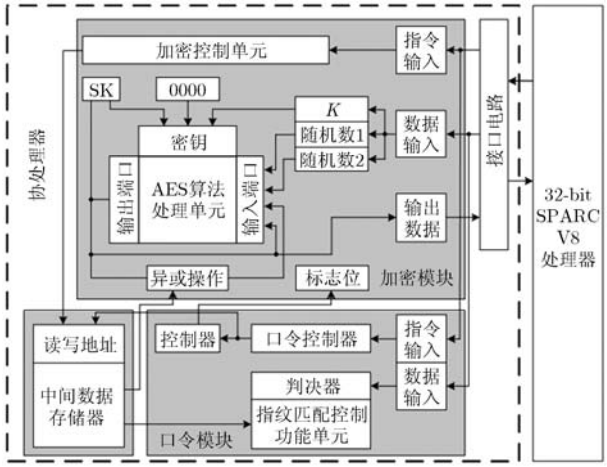


图 6 基于 WDDL 的 AES 密码算法协处理器

全协处理器芯片进行了防御 DPA 攻击的性能分析比较。对标准 CMOS 逻辑实现的 AES 算法，仅需要 8000 次功耗曲线样本就能实现 DPA 攻击；使用 WDDL 逻辑实现的 AES 算法使用 1500000 次功耗曲线样本时仍难实现 DPA 攻击。实验结果表明，WDDL 逻辑与标准 CMOS 逻辑相比较，在安全性方面至少可以提高 2 个数量级。

3.3 功耗扰乱技术

功耗扰乱技术包括时钟功耗扰乱技术和旁路功耗扰乱技术[5,55−59]。时钟功耗扰乱技术是指利用时钟频率的随机变化对密码芯片的微观功耗进行扰乱。韩军[5]提出基于时间随机化的密码芯片防御攻击方法，建立了随机时间延迟防御 DPA 攻击的理论模型，并得到了随机时间延迟抑制 DPA 攻击的阈值条件。文献[57]的分析结果表明，时钟功耗扰乱技术在提高芯片安全性的同时，会降低部分功耗，但造成约 16%时间损耗，影响数据处理性能。

旁路功耗扰乱技术是指在不影响系统性能的前提下，构建与密码算法关键模块相关的旁路模块，扰乱其功耗与数据的相关性，实现防御 DPA 攻击的目的。文献[56]针对 AES 密码算法关键模块 Sbox，提出如图 7 所示的旁路结构，其中旁路模块的电路结构为如图 8 所示的环形振荡器。该方法可以有效解决吞吐量退化问题。然而，在系统复位的时候伪随机数发生器生成数据字节是相同的，这就有可能被攻击者所利用。为了解决这个问题，文献[60]采用了真随机数发生器不仅能够自动生成随机数序列防御 DPA 攻击，而且可以在提高系统安全性的同时减少面积开销。

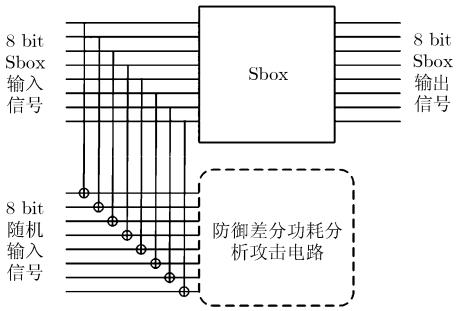


图 7 基于旁路功耗扰乱技术的 Sbox 结构框图

4 防御 DPA 攻击的前沿技术与发展趋势

上述主流防御 DPA 攻击方法并不完善，还存在以下方面的问题：Mask 技术需要增加屏蔽因子和掩码操作，改变了算法流程，并且在构造伪 Sbox 时往往需要十分大的硬件存储空间，这样就增加协处理器的面积；功耗平衡技术带来电路面积增大和平均功耗上升，另外硬件实现上需要全部重新设计，没有相应的自动化设计工具支持，比较费时费力；功耗扰乱技术能降低部分功耗，但通常会带来时间损

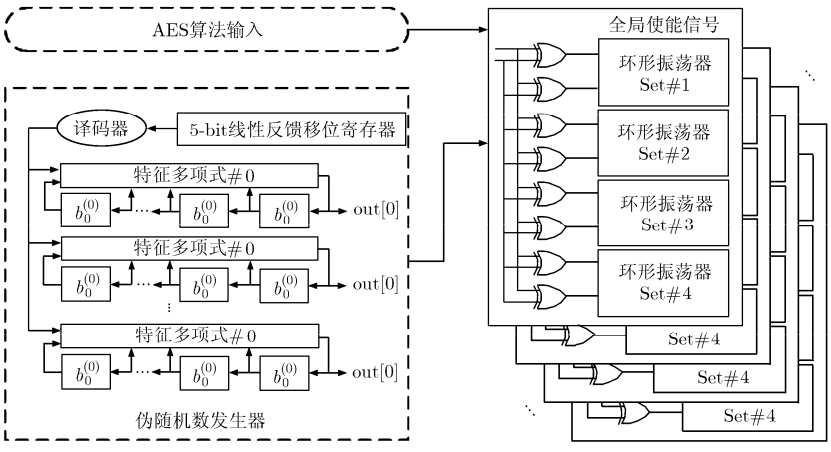


图 8 基于环形振荡器的旁路模块

耗，影响数据处理性能，增加额外面积开销。本节对未来可能产生重大影响的防御 DPA 攻击新技术进行探讨，包括基于物理不可克隆函数(PUF)电路的防御 DPA 技术、基于多值行为的防御 DPA 技术以及基于多核处理器的防御 DPA 技术等，同时探测防御 DPA 技术的发展新趋势和研究热点。

4.1 基于 PUF 电路的防御 DPA 攻击技术

PUF 最早由麻省理工大学的 Gassend 等人[61]提出，是一种半导体芯片的“芯片 DNA”技术，通过提取 IC 制造过程中不可避免产生的差异，生成无限多个唯一的、不可预测的密钥。这些密钥具有随机性、唯一性和不可克隆性等特性[62−72]。利用 PUF 电路的唯一性和不可克隆性，将芯片制造的工艺偏差与具体密码算法相融合，赋予电路输出的数据具有特定含义，实现电路功耗与所处理数据没有直接对应关系，使得攻击者无法获取真实信息。基于仲裁器和信号传输延迟的 PUF 方案是由一个信号传输延迟电路和一个仲裁器组成，如图 9 所示。电路中布置了上下两条完全对称的信号传输延迟通路，同一信号在两条通路上竞争通过，仲裁器根据竞争结果判断输出是 0 或 1。输入激励是一个 64 bit 的比特串，用来控制信号传输通路，输出是 1 bit，作为 PUF 的输出响应。可以将 PUF 电路应用到 AES 加密芯片，设计抗 DPA 攻击的 AES 芯片。

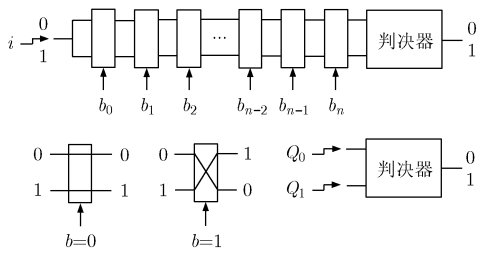


图 9 PUF 的电路结构

4.2 基于多值行为的防御 DPA 攻击技术

多值行为是指数字信号的取值数比传统的取值数 2(即 0、1)多的情况[73−77]。以四值为例(逻辑值为 0, 1, 2, 3)，逻辑值的数量为传统二值逻辑的两倍，输出端口逻辑状态跳变(0→0, 0→1, 0→2, 0→3, 1→0, 1→1, 1→2, 1→3, 2→0, 2→1, 2→2, 2→3, 3→0, 3→1, 3→2, 3→3)数为传统二值状态跳变(0→0, 0→1, 1→0, 1→1)数的 4 倍。随着基数的增加，状态跳变的复杂性呈指数形式增长。将多值行为融合到防御 DPA 攻击的 VLSI 设计中，利用多值行为状态跳变的多样性和复杂性，打破功耗与电路状态跳变之间的对应关系，达到提高电路安全性能的目的。同时，多值信号可以增加电路单线信息携带量，提高空间或时间的利用率，这将有利于提升密码芯片的性能。

4.3 基于多核处理器的防御 DPA 攻击技术

多核处理器的优势是每一个单核处理器都能以不同的时钟频率工作，结合时钟扰乱技术防御 DPA 攻击。另外，每个处理器的时钟可调，可以使得它工作在最佳的状态，任务多的时候就以接近满负荷的高时钟频率工作，达到最高的性能[78, 79]。Ambrose 等人[80−82]提出多核处理器在防御 DPA 攻击上的应用。基本思想是在越来越多处理器系统中利用功耗平衡的方法来防御 DPA 攻击，即每运行一条加密指令，两个结构完全相同的处理器单核，同时执行互补指令操作。当一个处理器开始执行加密算法时，自动启动第 2 个处理器的加密程序并执行互补指令，如图 10 所示。

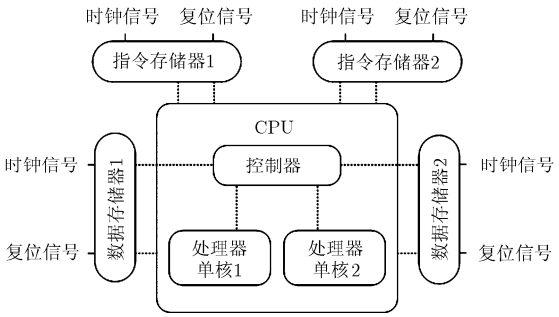
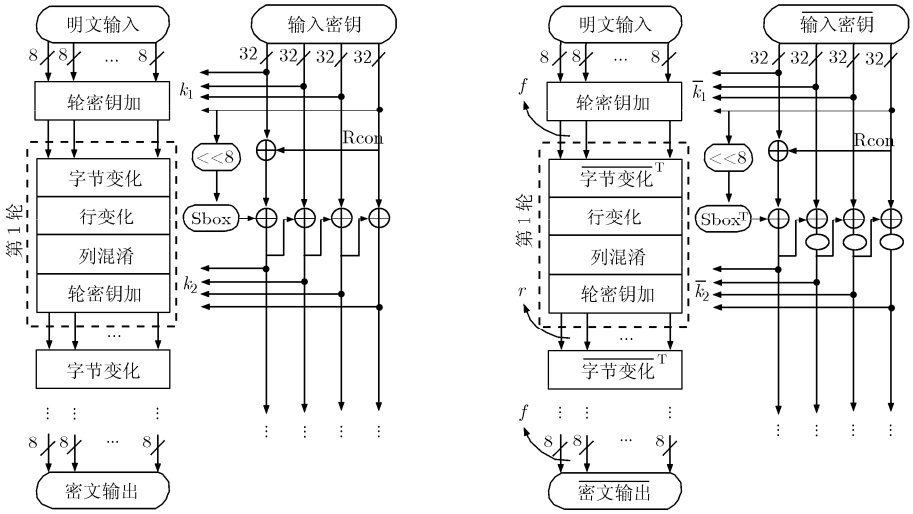


图 10 多核处理器的结构框图

多核处理器防御 DPA 攻击还需要设计相应的密码算法。文献[80]针对 AES 算法提出一种适用于多核处理器的功耗平衡算法。该设计具有两个显著的优点，一方面仅当 AES 算法执行时两个处理器才会进行平衡数据位翻转的操作，另一方面当加密电路不执行 AES 算法时，两个结构可分别执行独立的操作。MUTE-AES 算法结构如图 11 所示，包括 AES 加密算法与互补 AES 加密算法。同时该设计思想也可应用于数据加密标准算法(DES)，文献[81]提出适用于多核处理器的 MUTE-DES 算法，实现防御 DPA 攻击。

4.4 防御 DPA 攻击技术研究热点探讨

4.4.1 高性能、低成本的防御技术研究　目前，虽然已经提出不少防御 DPA 攻击技术，但是存在的主要问题是硬件成本太高，运算速度偏低，因此如何在确保安全性的同时提高密码芯片的性能，是未来防御 DPA 攻击技术研究的热点。半导体制造工艺的进步和市场的客观需求，也不断推动高性能、低成本防御技术的发展。Guo 等人[83]在权衡芯片面积、速度和安全性的前提下，提出一种通用椭圆曲线加密



(a)普通AES加密算法 (b)互补AES加密算法

图 11 MUTE-AES 加密算法

算法(ECC)协处理器架构，达到防御旁道攻击和故障攻击的目的。Cevrero 等人[48]提出通过 MCML 逻辑实现大大降低电路的功耗，达到低功耗防御功耗攻击设计，并建立 PG-MCML 的标准单元库，支持传统的电子设计自动化(EDA)工具。

4.4.2 防御复合型攻击技术研究 随着 DPA 攻击技术的研究使得密码芯片开始时刻面临复合型攻击的威胁。复合型攻击利用算法漏洞和旁道信息，综合数学攻击、功耗攻击、电磁辐射攻击、时间攻击、错误攻击和模板攻击等等技术，只要任何一个环节存在问题，都有可能造成关键信息泄露。所以它的攻击性更强，防御也更困难。Lejla 等人[84]集合碰撞攻击和 DPA 攻击，提出 DCA (Differential Cluster Analysis)攻击方法；Benedikt 等人[85]提出一种综合旁道泄露信息的 MIA(Mutual Information Analysis)攻击方法，并且 Nicolas 等人[86]对 MIA 攻击进行理论深化与可行性分析。目前关于防御复合型攻击的文献较少，有待学者进一步研究。

4.4.3 防御 DPA 攻击的测试平台 防御 DPA 攻击是一种实验性很强的技术手段，由于信息安全的特殊性，相关的测试技术和设备又受到国外限制，而目前国内的测试条件和实验设备相当有限，对大部分研究单位而言，防御 DPA 攻击技术的评价标准和评估手段基本停留在理论分析和软件仿真阶段。因此，制定有效的防御 DPA 攻击技术标准以及搭建防御 DPA 攻击测试平台，也是将来研究中必须解决的问题之一。

测试平台主要包括 DPA 测试平台的软件、硬件设计。软件方面需要包括集成各类数学模型的 DPA 数据分析软件，实验平台运行控制软件等；硬件方面需要包括集成加密芯片电路的硬件系统，功耗采集设备等。由 Tokyo Electron Device 公司提供的 SASEBO[87]是一款具有内置密码算法电路，专门为边旁道攻击设计的 FPGA 开发板，其中型号 SASEBO-GII 还增加了扩展外部实验设备的功能，如图 12 所示。它既可以提供密码算法的工作环境，又可以针对具体的密码算法实现旁道攻击，是一个小型测试平台。SASEBO-GII 配备最新的 Xilinx Virtex-5 LX30/LX50 FPGA 芯片用作算法电路，相比其它型号增加约 4～7 倍的逻辑电路面积；此外，它还向用户提供多种配置 FPGA 的途径，测试和用户界面大大简化。

关于防御 DPA 攻击技术还有以下几个方面值得关注：DPA 攻击及其防御技术理论有待进一步完善；功耗攻击技术与密码学等理论内在联系的研究有待于进一步深入；功耗安全策略等相关防御理论在密码芯片设计中有待进一步应用；防御系统的功

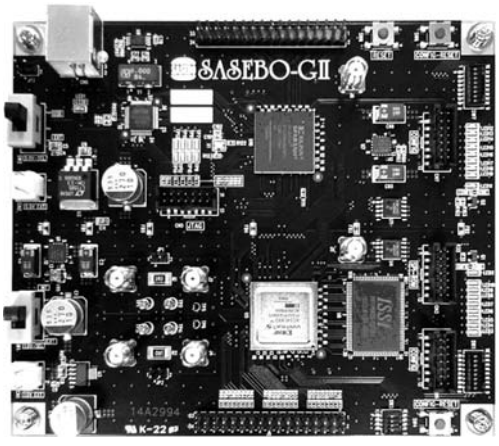


图 12 SASEBO-GII 开发板

耗、延时、面积等方面开销过大，电路结构有待进一步优化；防御系统性能评价缺乏统一的标准，基于功耗分析的相关度、2 维相关性等的安全性能评价体系有待充实完善。

5 结论

本文对防御 DPA 攻击技术进行了综述，对主流防御 DPA 攻击技术进行概述与分析，并对前沿防御技术与研究热点进行探讨。虽然对防御 DPA 攻击技术的研究已经取得一定的成果，但是存在的问题依然严峻，有待研究者进一步探索。密码芯片 DPA 防御技术研究是一个多学科交叉的工作，需要研究者具有现代密码学、数理统计学、电路与系统、微电子学等多种学科的知识，从数学分析、软件算法到电路结构，直至芯片 VLSI 实现都要有深入研究。并且此项研究还需要综合考虑多种因素，其中包括技术的因素，也包含社会和经济的因素。开展密码芯片的 DPA 防御技术研究，防止将来可能会出现的信息安全威胁，将对国民经济的健康发展和社会稳定繁荣起到良好的促进作用。

参 考 文 献

[1] Mangard S, Oswald E, and Popp T. Power Analysis Attacks: Revealing the Secrets of Smart Cards[M]. Graz University of Technology, Austria, Published by Springer, 2007: 1–306.

[2] Kocher P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[C]. Advances in Cryptology(CRYPTO'96), Berlin, Springer, 1996, LNCS 1109: 104–113.

[3] Kocher P C, Jaffe J, Jun B, *et al*.. Differential power analysis [C]. CRYPTO'99, Santa Barbara, CA, USA, Lecture Notes in Computer Science, Aug. 15–19, 1999: 388–397.

[4] Gandolfi K, Mourtel C, and Olivier F. Electromagnetic analysis: concrete results[C]. CHES 2001, 2001, LNCS 2162: 251–261.

[5] 韩军. 信息安全芯片的防御攻击技术研究[D]. [博士论文], 复旦大学, 2006.
Han Jun. Research on attack countermeasures of security chip [D]. [Ph.D. dissertation], Fundan University, 2006.

[6] 郑新建, 张翌维, 沈绪榜. SPA 和DPA 攻击与防御技术新进展[J]. 小型微型计算机系统, 2009, 30(4): 726–731.
Zheng Xin-jian, Zhang Yi-wei, and Shen Xu-bang. Advanced evolution of SPA and DPA attack and resistance techniques [J]. *Journal of Chinese Computer Systems*, 2009, 30(4): 726–731.

[7] Alioto M, Poli M, and Rocchi S. A general power model of differential power analysis attacks to static logic circuits [J]. *IEEE Transactions on Very Large Scale Integration* (*VLSI*) *Systems*, 2010, 18(5): 711–724.

[8] Wang Peng-jun and Hao Li-peng. A novel differential fault analysis on AES-128[C]. 2011 IEEE 9th International Conference on ASIC (ASICON), Xiamen, China, Oct. 25–28, 2011: 9–12.

[9] Lu Y, Boey K, Hodgers P, *et al*.. Lightweight DPA resistant solution on FPGA to counteract power models[C]. 2010 International Conference on Field-Programmable Technology (FPT), Beijing, China, Dec. 8–10, 2010: 178–183.

[10] Bodhisatwa M, Debdeep M, and Indranil S. Design for security of block cipher S-boxes to resist differential power attacks[C]. 2012 25th International Conference on VLSI Design (VLSID), Hyderabad, India, Jan. 7–11, 2012: 113–118.

[11] Mangard G. Securing implementations of block ciphers against side channel attacks[D]. [Ph.D. dissertation], Austria, Graz University of Technology, 2004.

[12] Oswald E, Mangard S, Pramstaller N, *et al*.. A side-channel analysis resistant description of the AES S-box[C]. 12th International Workshop Fast Software Encryption, 2005, LNCS 3557: 413–423.

[13] Kocher P. Design and validation strategies for obtaining assurance in countermeasures to power analysis and related attacks[C]. NIST Physical Security Workshop, San Francisco, America, 2005: 26–29.

[14] 汪鹏君, 郝李鹏, 张跃军. 防御零值功耗攻击的 AES SubByte 模块设计及其 VLSI 实现[J]. 电子学报, 2012, 40(11): 2183–2187.
Wang Peng-jun, Hao Li-peng, and Zhang Yue-jun. Design of AES subbyte module of anti-zero value power attack and its VLSI implementation[J]. *Acta Electronica Sinica*, 2012, 40(11): 2183–2187.

[15] Moradi A, Mischke O, and Paar C. Practical evaluation of DPA countermeasures on reconfigurable hardware [C]. 2011 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), San Diego, California, USA, June 5–6, 2011: 154–160.

[16] Bai Xue-fei, Huang Lu, Wang Yi-fei, *et al*.. Evaluation of DPA attack resistance of transistor-based adiabatic logic styles[C]. 2010 2nd International Conference on e-Business and Information System Security (EBISS), Wuhan, China, May 1–3, 2010: 22–23.

[17] 臧玉亮, 韩文报. 线性反馈移位寄存器的差分能量攻击[J]. 电子与信息学报, 2009, 31(10): 2406–2410.
Zang Yu-liang and Han Wen-bao. Differential power attack on liner feedback shift register[J]. *Journal of Electronics & Information Technology*, 2009, 31(10): 2406–2410.

[18] Michael Z, Michael K, Marc S, *et al*.. Side channel analysis of the SHA-3 finalists[C]. Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany, March 12–16, 2012: 1012–1017.

[19] Lin Lang and Burleson W. Analysis and mitigation of process variation impacts on power-attack tolerance[C]. 2009 47th ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, California, USA, July 2009: 26–31.

[20] Yoshikawa M and Sugiyama M. Multi-rounds masking method against DPA attacks[C]. 2011 IEEE International Conference on Information Reuse and Integration (IRI), Las Vegas, USA, Aug. 3–5, 2011: 100–103.

[21] Yoshikawa M and Kojima Y. Efficient random number for the masking method against DPA attacks [C]. 2011 21st International Conference on Systems Engineering (ICSEng), Las Vegas, USA, Aug. 16–18, 2011: 321–324.

[22] Zhang Tao, Fan Ming-yu, and Zheng Xiao-yu. Secure and efficient elliptic curve cryptography resists side-channel attacks[J]. *Journal of Systems Engineering and Electronics*, 2009, 20(3): 660–665.

[23] Prouff E and McEvoy R. First-order side-channel attacks on the permutation tables Countermeasure[C]. CHES 2009, 2009, LNCS 5747: 81–96.

[24] 赵佳, 曾晓洋, 韩军, 等. 抗差分功耗分析攻击的 AES 算法的 VLSI 实现[J]. 计算机研究与发展, 2007, 44(3): 378–383.
Zhao Jia, Zeng Xiao-yang, Han Jun, *et al.*. VLSI implementation of an AES algorithm resistant to differential power analysis attack[J]. *Journal of Computer Research and Development*, 2007, 44(3): 378–383.

[25] 郑新建, 张翌维, 彭波, 等. 抗 DPA 攻击的 AES 算法研究与实现[J]. 计算机科学与探索, 2009, 3(4): 405–412.
Zheng Xin-jian, Zhang Yi-wei, Peng Bo, *et al.*. Research and implementation of DPA resistant AES algorithm [J]. *Journal of Frontiers of Computer Science and Technology*, 2009, 3(4): 405–412.

[26] Gebotys C H. A table masking countermeasure for low-energy secure embedded systems[J]. *IEEE Transactions on Very Large Scale Integration* (*VLSI*) *Systems*, 2006, 14(7): 740–753.

[27] Alam M, Ghosh S, Mohan M J, *et al.*. Effect of glitches against masked AES S-box implementation and countermeasure[J]. *IET Information Security*, 2009, 3(1): 34–44.

[28] Fischer W and Gammel B M. Masking at gate level in the presence of glitches[C]. CHES 2005, 2005, LNCS 3659: 187–200.

[29] Popp T and Mangard S. Masked dual-rail pre-charge logic: DPA-resistance without routing constraints [C]. CHES 2005, 2005, LNCS 3659: 172–186.

[30] Rivain M and Prouff E. Provably secure higher-order masking of AES[C]. CHES 2010, 2010, LNCS 6225: 413–427.

[31] Coron J S, Prouff E, and Rivain M. Side channel cryptanalysis of a higher order masking scheme[C]. CHES 2007, 2007, LNCS 4727: 28–44.

[32] Rivain M, Prouff E, and Doget J. Higher order masking and shuffling for software implementations of block ciphers[C]. CHES 2009, 2009, LNCS 5747: 171–188.

[33] 童元满, 王志英, 戴葵, 等. 一种抗 DPA 及 HO-DPA 攻击的 AES 算法实现技术[J]. 计算机研究与发展, 2009, 46(3): 377–383.
Tong Yuan-man, Wang Zhi-ying, Dai Kui, *et al.*. A DPA and HO-DPA resistant implementation of AES[J]. *Journal of Computer Research and Development*, 2009, 46(3): 377–383.

[34] Najeh K, Lilian B, and Adel G. A masked correlated power noise generator use as a second order DPA countermeasure to secure hardware AES cipher[C]. 2011 23rd International Conference on Microelectronics (ICM), Hammamet, Tunisia, Dec. 19–22, 2011: 1–5.

[35] Kim Hee-Seok, Hong Seo-khie, and Lim Jongin. A fast and provably secure higher-order masking of AES S-box [C]. CHES 2011, 2011, LNCS 6917: 95–107.

[36] Fumaroli G, Martinelli A, Prouff E, *et al.*. Affine masking against higher-order side channel analysis[C]. CHES 2011, 2011, LNCS 6917: 262–280.

[37] Yue Da-heng, Li Shao-qing, and Zhang Min-xuan. Static timing analysis in dual-rail precharge logic based DPA resistant circuit design[C]. 2010 International Conference on Electronics and Information Engineering (ICEIE), Sichuan, China, Aug. 1–3, 2010: V1-236–V1-240.

[38] Bucci M, Giancane L, Luzzi R, *et al.*. Delay-based dual-rail precharge logic[J]. *IEEE Transactions on Very Large Scale Integration* (*VLSI*) *Systems*, 2011, 19(7): 1147–1153.

[39] Guilley S, Sauvage L, Flament F, *et al.*. Evaluation of power constant dual-rail logics countermeasures against DPA with design time security metrics[J]. *IEEE Transactions on Computers*, 2010, 59(9): 1250–1263.

[40] Zhang Yue-jun, Wang Peng-jun, and Hao Li-peng. Design of resistant DPA three-valued counter based on SABL [C]. 2011 IEEE 9th International Conference on ASIC (ASICON), Xiamen, China, Oct. 25–28, 2011: 9–12.

[41] Hwang T D and Hodjat A. AES based cryptographic and biometric security coprocessor IC in 0.18 μm CMOS resistant to side-channel power analysis attacks [J]. *IEEE Transactions on Journal of Solid-State Circuits*, 2006, 41(4): 781–792.

[42] Bucci M, Giancane L, Luzzi R, *et al.*. Three-phase dual-rail pre-charge logic[C]. CHES 2006, 2006, LNCS 4249: 232–241.

[43] Sokolov D, Murphy J, Bystrov A, *et al.*. Design and analysis of dual-rail circuits for security applications[J]. *IEEE Transactions on Computers*, 2005, 54(4): 449–459.

[44] Suzuki D and Saeki M. Security evaluation of DPA countermeasures using dual-rail pre-charge logic style[C]. CHES 2006, 2006, LNCS 4249: 255–269.

[45] Atani R E, Mirzakuchaki S, Atani S E, *et al*.. Design and simulation of a DPA resistive circuit for tritium stream cipher based on SABL Logic styles[C]. 15th International Conference on Mixed Design of Integrated Circuits and Systems (MIXDES 2008), Pozna, Poland, 2008: 19–21.

[46] Renauld M, Kamel D, Standaert F, *et al*.. Information theoretic and security analysis of a 65-nanometer DDSLL AES S-box [C]. CHES 2011, 2011, LNCS 6917: 223–239.

[47] Iwai K, Shiozaki M, Hoang A T, *et al*.. Implementation and verification of DPA-resistant cryptographic DES circuit using Domino-RSL[C]. 2011 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), San Diego, California, USA, June 5–6, 2011: 28–33.

[48] Cevrero A, Regazzoni F, Schwander M, *et al*.. Power-gated MOS current mode logic (PG-MCML): a power aware DPA-resistant standard cell library[C]. 2011 48th ACM/EDAC/IEEE Design Automation Conference (DAC), San Diego, California, USA, June 5–9, 2011: 1014–1019.

[49] Djukanovic M, Giancane L, Scotti G, *et al*.. Leakage power analysis attacks: effectiveness on DPA resistant logic styles under process variations[C]. 2011 IEEE International Symposium on Circuits and Systems (ISCAS), Rio de Janeiro, Brazil, May 15–18, 2011: 2043–2046.

[50] Mangard S, Oswald E, and Standaert F X. One for all-all for one: unifying standard differential power analysis attacks [J]. *IET Information Security*, 2011, 5(2): 100–110.

[51] Burns F, Bystrov A, Koelmans A, *et al*.. Design and security evaluation of balanced 1-of-n circuits[J]. *IET Computers & Digital Techniques*, 2012, 6(2): 125–135.

[52] Maxime N, Youssef S, Sylvain G, *et al*.. RSM: a small and fast countermeasure for AES, secure against 1st and 2nd-order zero-offset SCAs[C]. 2012 Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany, March 12–16, 2012: 1173–1178.

[53] Liu Po-chun, Hsiao Ju-hung, Chang Hsie-chia, *et al*.. A 2.97 Gb/s DPA-resistant AES engine with self-generated random sequence[C]. 2011 Proceedings of the ESSCIRC (ESSCIRC), Helsinki, Finland, Sept. 12–16, 2011: 71–74.

[54] Ratanpal G B, Williams R D, and Blalock T N. An on-chip signal suppression countermeasure to power analysis attacks [J]. *IEEE Transactions on Dependable and Secure Computing*, 2004, 1(3): 179–188.

[55] Rakers P, Connell L, Collins T, *et al*.. Secure contactless smartcard ASIC with DPA protection[J]. *IEEE Transactions on Journal of Solid-State Circuits*, 2001, 36(3): 559–565.

[56] Liu Po-chun, Chang Hise-chia, and Lee Chen-yi. A low overhead DPA countermeasure circuit based on ring oscillators[J]. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2010, 57(7): 546–550.

[57] Bucci M, Luzzi R, and Guglielmo M. A countermeasure against differential power analysis based on random delay insertion[C]. 2005 IEEE International Symposium on Circuits and Systems, Kobe, Japan, May 2005: 3547–3550.

[58] Regazzoni F, Cevrero A, and Standaert F X. A design flow and evaluation framework for DPA-resistant instruction set extensions[C]. CHES 2009, 2009, LNCS 5747: 205–219.

[59] Tillich S and Groch A J. Power analysis resistant AES implementation with instruction set extensions [C]. CHES 2007, 2007, LNCS 4727: 303–319.

[60] Liu Po-chun, Chang Hise-chia, and Lee Chen-yi. A true random-based differential power analysis countermeasure circuit for an AES engine[J]. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2012, 59(2): 103–107.

[61] Gassend B, Clarke D, Marten V D, *et al*.. Silicon physical random functions[C]. Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington, DC, USA, 2002: 148–160.

[62] Pappu R, Recht B, Taylor J, *et al*.. Physical one-way functions[J]. *Science*, 2002, 297(5589): 2026–2030.

[63] Lim D and Lee J W. Extracting secret keys from integrated circuits[J]. *IEEE Transactions on VLSI Systems*, 2005, 13(10): 1200–1205.

[64] Zhang Yue-jun, Wang Peng-jun, Li Yi, *et al*.. Model and physical implementation of multi-port PUF in 65nm CMOS [J]. *International Journal of Electronics*, 2012 (online).

[65] Suh G E and Devadas D. Physical unclonable functions for device authentication and secret key generation[C]. Design Automation Conference, San Diego, California, USA, 2007: 9–14.

[66] Edward G S and Devadas S. Physical unclonable functions for device authentication and secret key generation [C]. DAC 2007, San Diego, California, USA, 2007: 9–14.

[67] Holcomb D E, Burleson W P, and Fu K. Power-up SRAM state as an identifying fingerprint and source of true random numbers[J]. *IEEE Transactions on Computers*, 2009, 58(9): 1198–1210.

[68] Guajardo J, Kumar S S, Schrijen G J, *et al*.. FPGA intrinsic PUFs and their use for IP protection [C]. CHES 2007, 2007, LNCS 4727: 63–80.

[69] Kumar S and Guajardo J. The butterfly PUF protecting IP on every FPGA[C]. IEEE International Workshop on Host, Anaheim, CA, USA, 2008: 67–70.

[70] Lin L and Burleson W. Analysis and mitigation of process variation impacts on power-attack tolerance[C]. DAC 2009, San Francisco, California, USA, 2009: 26–31.

[71] Majzoobi M, Koushanfar F, and Potkonjak M. Techniques for design and implementation of secure reconfigurable PUFS [J]. *ACM Transactions on Reconfigurable Technology and*

Systems, 2009, 2(1): 1–33.

[72] Suzuki D and Shimizu K. The glitch PUF: a new delay-PUF architecture exploiting glitch shapes [C]. CHES 2010, 2010, LNCS 6225: 366–382.

[73] 吴训威. 多值逻辑电路设计原理[M]. 杭州: 杭州大学出版社, 1994: 18–55.
Wu Xun-wei. Design principles of multivalued logic circuits [M]. Hangzhou: Publishing of Hangzhou University Press, 1994: 18–55.

[74] Wang Peng-jun and Zhang Yue-jun. Design of four-valued operation circuits of adder and subtraction based on neuron MOS transistor[C]. 2009 Asia-Pacific Conference Information Processing, Shenzhen, China, 2009: 382–385.

[75] Zhang Yue-jun and Wang Peng-jun. Design of multi-valued double-edge-triggered JK flip-flop based on neuron MOS transistor[C]. 2009 IEEE 8th International Conference on ASIC, Changsha, China, 2009: 58–61.

[76] Wang Peng-jun, Li Kun-peng, and Mei Feng-na. Design of a DTCTGAL circuit and its application[J]. *Journal of Semiconductors*, 2009, 30(11): 115006-1–115006-6.

[77] Wang Peng-jun and Gao Hong. Design of novel QCTGAL circuit[C]. 2010 10th IEEE International Conference on Solid-State and Integrated Circuit Technology Proceedings, Shanghai, China, 2010: 680–683.

[78] Yu Z Y, Michael J M, Ryan W A, *et al*.. AsAP: an asynchronous array of simple processors [J]. *IEEE Transactions on Journal of Solid-State Circuits*, 2006, 43(3): 695–705.

[79] Yu Z Y, You K D, Xiao R J, *et al*.. An 800 MHz 320 mW 16-core processor with message-passing and shared-memory inter-core communication mechanisms[C]. 2012 IEEE International Solid-State Circuits Conference Digest of Technical Papers(ISSCC), San Francisco, CA, USA, Feb. 19–23, 2012: 64–66.

[80] Ambrose J A, Parameswaran S, and Ignjatovic A. MUTE-AES: a multiprocessor architecture to prevent power analysis based side channel attack of the AES algorithm [C]. 2008 IEEE/ACM International Conference on Computer-Aided Design, San Jose, CA, USA, Nov. 10–13, 2008: 678–684.

[81] Ambrose J A. Power analysis side channel attacks: the processor design-level context[D]. [Ph.D. dissertation], University of New South Wales, 2009.

[82] Ambrose J A, Ragel R G, Parameswaran S, *et al*.. Multiprocessor information concealment architecture to prevent power analysis-based side channel attacks [J]. *IET Computers & Digital Techniques*, 2011, 5(1): 1–15.

[83] Guo X, Fan J F, Schaumont P, *et al*.. Programmable and parallel ECC coprocessor architecture: tradeoffs between area, speed and security[C]. CHES 2009, 2009, LNCS 5747: 289–303.

[84] Lejla B, Benedikt G, and Kerstin L R. Differential cluster analysis[C]. CHES 2009, 2009, LNCS 5747: 112–127.

[85] Benedikt G, Lejla B, Pim T, *et al*.. Mutual information analysis: a generic side-channel distinguisher[C]. CHES 2008, 2008, LNCS 5154: 426–442.

[86] Nicolas V C and Standaert F X. Mutual information analysis: how, when and why?[C]. CHES 2009, 2009, LNCS 5747: 429–443.

[87] Side-channel attack standard evaluation board [CL]. http://www.inrevium.jp/eng/ sasebog2_user/, 2009.

汪鹏君： 男，1966 年生，教授，博士生导师，研究方向为低功耗集成电路理论和设计技术、高信息密度集成电路理论和设计技术、安全芯片理论和设计技术、电路设计综合和优化技术、多媒体技术以及相关理论.

张跃军： 男，1982 年生，博士生，研究方向为密码芯片攻击和防御理论及其 VLSI 实现、多值逻辑电路理论和设计技术.

张学龙： 男，1988 年生，硕士生，研究方向为密码芯片攻击和防御理论及其 VLSI 实现、多值逻辑电路理论和设计技术.