文章编号: 1001- 2486(2009) 06- 0018- 07

基于 LBDL 逻辑的抗 DPA 攻击电路设计方法*

乐大珩, 李少青, 张民选
(国防科技大学 并行与分布处理国防科技重点实验室, 湖南 长沙 410073)

摘 要: 动态差分逻辑是一种典型的电路级差分功耗攻击(DPA)防护技术。这种技术通过使逻辑门保持恒定的翻转率来降低电路功耗与数据信号之间的相关性。介绍了一种新型的、基于查找表(Look-Up-Table, LUT)结构的动态差分逻辑(LBDL), 以及基于这种逻辑的集成电路设计方法。该设计方法仅需在传统的半定制设计流程中添加少量的替换操作就可以实现, 因而比其他完全需要全定制设计的动态差分逻辑具有更好的实用性。而相对同样适用于半定制实现的动态差分逻辑 WDDL(Wave Dynamic Differential Logic), LBDL 逻辑解决了逻辑门翻转时刻与数据信号之间的相关性, 从而比 WDDL 逻辑具有更好的功耗恒定性。实验结果表明, 该设计方法能够有效实现具有抗 DPA 攻击性能的电路。

关键词: 安全芯片; DPA 攻击; 动态差分逻辑
中图分类号: TN431.2 文献标识码: A

An LBDL Based VLSI Design Method to Counteract DPA Attacks

YUE Da-heng, LI Shao-qing, ZHANG Min-xuan
(Parallel and Distributed Processing Laboratory, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: Dynamic and differential logic styles are proposed as a typical differential power analysis (DPA) resistant technology. Because of the constant transition rate of dynamic and differential logic gates, the correlation between power consumption and signal values is significantly reduced. In this paper, a novel look-up-table (LUT) based differential logic (LBDL) and the design method based on this logic are presented. Instead of a full custom design, this method combines some modification with a regular standard cell design flow. Thus, have a better practicability. Unlike WDDL (Wave Dynamic Differential Logic), which can also be implemented by standard cell design flow, the transition time of LBDL gates is independent of input values, hence power consumption of LBDL is more constant. Experimental results indicate that the LBDL-based design method can eliminates most of the power leakage.

Key words: security chip; DPA attack; dynamic and differential logic

当前主流的集成电路设计都是基于静态互补 CMOS 逻辑实现的。在这种电路中, 电路的动态功耗与其处理的数据具有密切的相关性。基于这一特点, P. Kocher 等提出了针对安全芯片的差分功耗分析(Differential Power Analysis, DPA)技术[1]。这种攻击技术避开了传统数学理论攻击的复杂性, 大大降低了密钥破解难度, 对安全芯片造成重大威胁。因此, 自从 DPA 攻击技术在 1999 年被提出以来, 不断有研究者提出针对这种攻击的防护技术。电路级的 DPA 防护技术研究主要在于设计新型的电路逻辑和电路工作方式, 从根本上去除电路工作功耗与其所处理数据之间的相关性。由于其所关注的是电路结构而不是密码算法, 因此电路级的 DPA 防护技术具有更好的通用性和安全性, 一旦有效且实用的防护结构被提出, 就可以保证各种密码算法的安全性。

在现有被提出的电路级防护技术中, 动态差分逻辑是一种比较有效的结构。比如 Kris Tiri 等提出的 SABL(Sense Amplifier Based Logic)逻辑[2]、WDDL(Wave Dynamic Differential Logic)逻辑[3-4], F. Mace 等提出的 DyCML(Dynamic Current Mode Logic)逻辑[5], M. Bucci 等提出的 TDPL(Three-Phase Dual-Rail Pre-charge Logic)逻辑[6], 以及 T. Popp 等提出的 MDPL(Masked Dual Rail Pre-charge Logic)逻辑[7]等。这些逻

* 收稿日期: 2009- 07- 03
基金项目: 国家自然科学基金资助项目(60873016); 国家 863 计划资助项目(2009AA01Z102); 教育部"高性能微处理器技术"创新团队资助项目(IRT0614)
作者简介: 乐大珩(1980—), 男, 博士生。

辑结构的特点是将传统的静态 CMOS 逻辑单元替换为具有双端差分输出的逻辑单元,同时采用了动态逻辑的预充电和求值操作,从而保证逻辑单元在每个时钟周期都具有固定的、与处理数据无关的信号翻转率。这样,在满足两个差分输出端负载相同的情况下就可以实现逻辑单元具有与所处理的数据无关的恒定功耗。在上述逻辑中,SABL、DyCML 和 TDPL 逻辑是全新设计的动态电路,具有很好的功耗恒定特性,但只能采用全定制的设计方法实现,难以与已有的集成电路设计流程结合。而且每个动态逻辑单元都需要精确设计的预充电控制信号,增大了芯片电路的设计难度。而在 WDDL 和 MDPL 逻辑中,研究者采用已有的标准单元搭建动态差分逻辑。在基于这些逻辑设计芯片电路时,仅需要对传统的半定制设计流程进行适量修改就可以实现[3-4,8]。但由于 WDDL 和 MDPL 逻辑采用已有的标准单元搭建,对可以使用的逻辑单元功能有很大限制;而且标准单元信号翻转时刻随输入信号取值的变化使得这些逻辑的功耗与所处理的数据之间仍然存在一定的相关性,这也降低了芯片的抗 DPA 攻击性能[9-10]。

基于上述分析,本文提出了一种新型的动态差分逻辑结构 LBDL(Look-Up-Table Based Differential Logic)。一方面,这种逻辑采用了定制设计的逻辑结构作为基本功能单元,具有良好的功耗恒定特性,同时还解决了 WDDL 逻辑中存在的单元翻转时刻与所处理的数据相关的问题。另一方面,LBDL 逻辑能够较好地适用于传统的电路综合和布局布线流程,与需要完全采用全定制设计的逻辑相比,具有更好的实用性。

1 LBDL 逻辑结构

LBDL 逻辑是基于 WDDL 逻辑思想提出的一种新型的动态差分逻辑,在 LBDL 逻辑中采用了查找表(Look-Up-Table, LUT)作为基本功能单元,因而解决了在 WDDL 逻辑中单元输出端翻转时刻与输入数据取值的相关性问题。

1.1 基本单元

图 1 所示是 LBDL 逻辑的基本结构,其中基本逻辑单元采用了 LUT 结构。(a)图所示是基于 LUT 的两输入与逻辑结构,左边的 VDD 和 GND 端表示了与逻辑的函数值,6 个 NMOS 管构成了 LUT 的译码器,反相器作为输出端负载的驱动单元。当输入端接收到互补的输入信号时,相应的 NMOS 管被打开,将 VDD 或 GND 连接到反相器的输入端,从而通过反相器输出逻辑值。比如当 a 和 b 的正、负信号端都接收到互补的(1,0)信号时,电路中最下端的两个 NMOS 管将反相器的输入连接到 GND,使反相器输入逻辑值 1。当输入端接收到另外的差分输入信号时,逻辑单元则会输出逻辑值 0。

为了实现 LBDL 逻辑的预充电功能,除了基本的 LUT 结构外,我们还添加了 6 个 PMOS 管作为预充电逻辑。在预充电阶段,单元正、负输入端都将接收到 0 信号。此时,PMOS 管同时导通,将反相器的输入端充电为高,使其输出 0 信号,而输出的 0 信号又会使下一级单元进入预充电状态。LBDL 逻辑采用专门的 PMOS 管实现预充电行为,这与 WDDL 逻辑中利用与门和或门的逻辑特性实现预充电功能不同。因此,在 LBDL 逻辑中,对基本单元的逻辑功能没有限制。

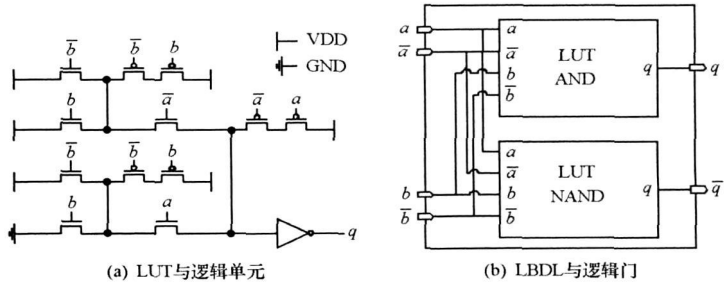

图 1 LBDL 逻辑门结构

Fig. 1 Components of LBDL

对图 1(a)所示的 LUT 逻辑单元,不论是在预充电阶段还是在求值阶段都最多只会发生一次翻转,

即在预充电阶段只可能发生($1\rightarrow 0$)翻转,而在求值阶段只可能发生($0\rightarrow 1$)翻转。这样,图 1(b)所示的 LBDL 逻辑门就具有动态差分逻辑的特点。从图中可以看出,每个 LBDL 逻辑门由两个 LUT 逻辑单元构成。其中一个 LUT 单元输出逻辑门的正信号,而另一个 LUT 单元输出负信号。在预充电阶段,输入端接收的全 0 信号将正、负输出端都预充到 0。在求值阶段,当输入端接收到了互补的差分信号后,两个 LUT 单元中只会有一个发生 0 到 1 的跳变。由此可见,在每个时钟周期 LBDL 逻辑门都必然有且仅会有一个输出端发生翻转,即 LBDL 逻辑门具有恒定的与输入取值无关的信号翻转率。

LUT 逻辑单元的另一特点是只要替换图 1(a)中 VDD 和 GND 的位置,就可以利用相同的电路结构实现任意功能的两输入逻辑,这样有利于降低建立 LBDL 逻辑单元库的难度。图 2 所示为两输入的 LBDL 与逻辑门版图,只要修改 VDD 和 GND 的连接关系就可以生成其他功能的两输入逻辑门。

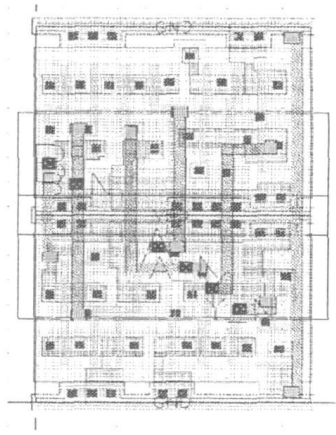

图 2 LBDL 两输入与逻辑门版图
Fig. 2 Layout of LBDL 2-input AND gate

与 WDDL 和 MDPL 等动态差分逻辑相比,除了恒定的信号翻转率外,LBDL 逻辑还具有单元输出端翻转时刻与输入信号取值无关的优点。在基于标准单元实现的集成电路中,逻辑单元各输入端信号的传输延迟通常是不同的。在这种情况下,对于 WDDL 逻辑和 MDPL 逻辑,到达时间较早的输入信号取值通常就决定了该单元输出端的翻转时刻。比如对于两输入的 WDDL 与门,如果较早到达的输入信号逻辑值为 0,则该逻辑门的负输出端会在此刻开始发生从 0 到 1 的跳变;而如果较早到达的输入信号逻辑值为 1,则该逻辑门要等到较晚的输入信号到达才开始翻转。由于集成电路工作时某一时刻的动态功耗等于此刻电路中所有正在翻转的逻辑门动态功耗的总和,因此,在 WDDL 逻辑和 MDPL 逻辑中,逻辑门翻转时刻随输入信号取值的变化会造成电路功耗与所处理数据的相关性。而对于 LBDL 逻辑,由于 LUT 单元的结构特点,使得逻辑门的翻转时刻与输入端信号的取值无关。从图 1 中可以看出,在求值阶段,只有当所有输入端的差分信号到达后 LUT 单元的输出端才会发生 0 到 1 的跳变;而在预充电阶段,一旦有一个输入端接收到了全 0 信号,LUT 单元的输出端就会发生翻转。这样,无论输入信号的取值如何,LBDL 逻辑门都具有固定的翻转时刻。在下一节的 SPICE 模拟分析中可以看出,LBDL 逻辑的这一特性使其相对于 WDDL 逻辑具有更好的功耗恒定性。

1.2 功耗恒定性分析

为验证 LBDL 逻辑功耗的恒定性,我们对一个两输入 LBDL 与门进行了 SPICE 模拟。我们使用 Kris Tiri 提出的标准功耗偏差 NED(Normalized Energy Deviation)作为 LBDL 逻辑功耗恒定性的量化评估[2]。通过模拟我们得到两输入 LBDL 与门的 NED 为 5.12%,相对于传统 CMOS 逻辑门减小了 94.7%。

为了验证逻辑门翻转时刻随输入信号取值变化对电路功耗的影响,我们分别对 WDDL 逻辑和 LBDL 逻辑的两输入与门进行了 SPICE 模拟分析,并通过在逻辑门的两个输入端插入不同的延迟单元实现输入端信号到达时刻的差异。在分析过程中,我们首先对两种与逻辑门进行了全部 4 种输入情况的 SPICE 模拟,然后根据延迟较短的输入信号的取值不同,将模拟得到的功耗曲线划分为两组并分别得到平均功耗曲线,如图 3 所示。

从图中可以看出,对于 WDDL 逻辑与门,当延迟较短的输入信号取值分别为 1 和 0 时,电路的平均功耗曲线表现出不同的形状;而对于 LBDL 逻辑,由于 LUT 门翻转时刻不随输入端信号取值而变化,使得两条平均功耗曲线几乎完全一致。由此可见,LBDL 逻辑比 WDDL 逻辑具有更好的功耗恒定性。

2 基于 LBDL 的电路设计

由于动态差分逻辑单元采用的是双端差分信号作为输入和输出,无法直接用现有的 EDA 工具设计实现,因此本文采用了一种基于差分布线方法的半定制设计流程[3],如图 4 所示。其主要思想是在传统的 ASIC 半定制设计流程中加入单元替换和差分布线步骤。

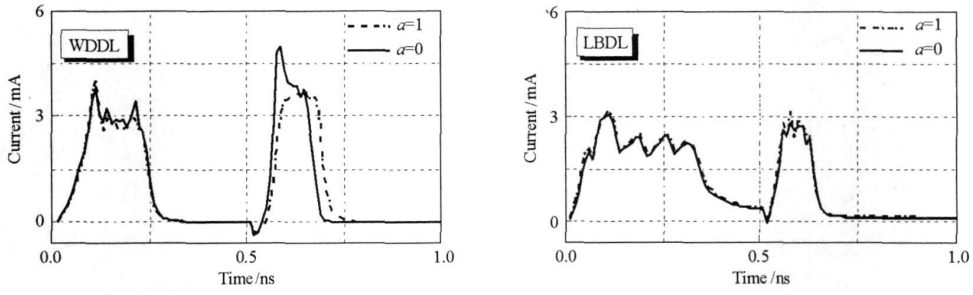

图 3 两输入与门的平均功耗曲线

Fig. 3 Current trace of AND gates

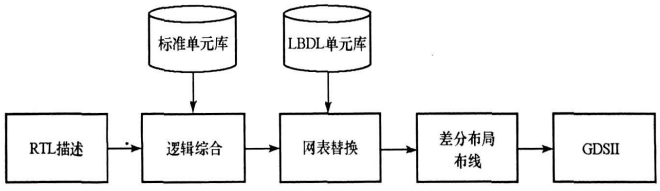

图 4 基于LBDL 逻辑的芯片设计流程

Fig. 4 LBDL based design flow

由于商用的 EDA 综合工具无法直接处理具有差分输入、输出功能的标准单元,因此在图 4 所示的流程中,首先需要将代码级的设计描述映射为商用标准单元库下的门级网表,然后再通过网表替换操作将网表中的所有标准单元替换为LBDL 逻辑库中的对应功能单元,并且建立单元正、负信号端的连接关系。

虽然LBDL 逻辑单元具有恒定的信号翻转率和翻转时刻,但要实现电路的功耗恒定还必须保证所有单元的正、负输出端具有完全相同的电容负载。要实现这一目的就需要所有差分信号的正、负信号线具有完全相同的布线结构。现有的 EDA 布局布线工具无法进行这样的布线操作,因此必须采用对信号线复制和平移的方法来实现差分布线。

差分布线方法的基本思想是首先将电路看作是只有正信号的单端电路,并利用 EDA 工具完成对正信号的布线,然后再将正信号线复制和平移得到负信号线的布线结构。这样,电路中所有的正、负信号线就具有了完全相同的布线结构[11]。为了避免信号线在复制和平移后发生最小间距的违反,甚至发生信号线的重叠短路,在进行单端布线时必须保证布线轨道具有 2 倍的标准布线间距。因此,为实现差分布线,LBDL 逻辑单元库需要为布局布线工具提供 2 套 LEF 文件。在用于单端布线的LEF 文件 single. lef 中,每个逻辑单元只包含正的输入、输出引脚信息,且布线轨道间距设置为标准间距的 2 倍。而另一套 LEF 文件 diff. lef 则用于对差分布线结果的规则检查和生成最终版图,其中包含了逻辑单元所有正、负引脚信息,且布线轨道间距设置为标准间距。同样道理,在之前的网表替换操作中,也需要提供两套门级网表: single. v 和 diff. v。其中网表 single. v 只包含正信号的连接关系,而网表 diff. v 则包含所有差分信号的连接关系。

差分布线的基本流程如图 5 所示。在初始阶段,EDA 工具首先读入 single. lef 文件和网表 single. v,通过自动布局布线得到只有正信号线的布线结构,如图 6 中左图所示,并且将布线后的信息保存成 DEF 文件 single. def。在 DEF 文件中,所有信号线的位置和长度是通过连线两端点的坐标描述的。因此只要将 single. def 中所有连线的坐标复制并沿 x 和 y 方向平移一个布线格点长度就能够得到负信号线。由于布局布线工具的工作特点,双倍间距的布线轨道与标准间距的布线轨道间存在半个布线格点长度的偏移,因此在实际的复制和平移操作中是将原有信号线同时向坐标轴的正、负方向偏移半个布线格点得到正、负信号线。连线的复制和平移操作生成包含差分布线结构的 diff. def 文件,将其与包含差分信号

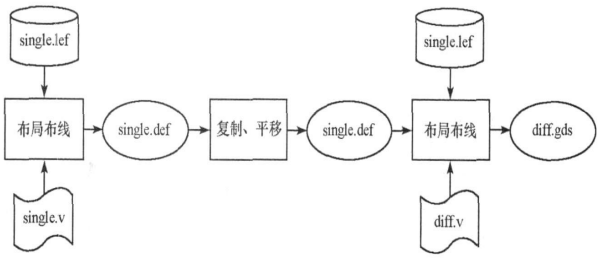

图5 差分布局布线流程

Fig. 5 Differential place-and-route flow

的网表 diff. v 以及文件 diff. lef 重新导入布局布线工具就可得到实际的差分布线结构, 如图 6 中右图所示。从图中可以看出, 所有的正、负信号线都具有完全相同的布线结构, 即都具有几乎相同的布线环境, 这样就保证了每对差分信号线都具有对称的电容负载。通过对导出的含连线寄生参数的版图 SPICE 网表进行统计分析, 差分布线方法得到的正、负信号线间电容负载差异不超过 1fF。

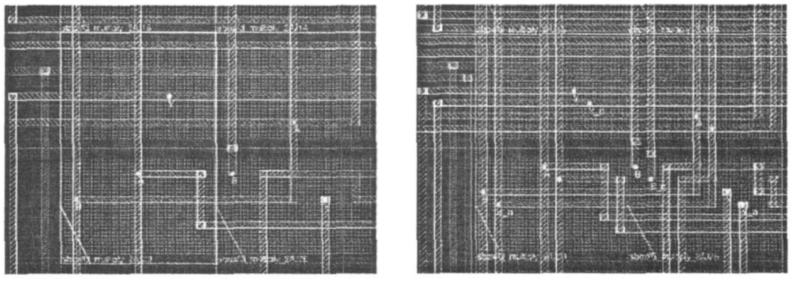

图6 单端布线(左)和差分布线(右)

Fig. 6 Single route (left) and differential route (right)

3 实验与模拟

为验证本文所提出的基于 LBDL 逻辑的电路设计方法对 DPA 攻击的防护效果, 我们在 0. 18μm 工艺下实现了如图 7 所示的 DPA 攻击模型电路。所采用的模型电路是 AES 密码算法最后一轮变换操作的电路子集。将算法电路作此简化是为了能够实现晶体管级的 SPICE 模拟, 从而得到精确的电路功耗数据。在模型电路中, 8bit 的输入数据经过 SBOX 变换后与轮密钥(Round Key)的 8bit 进行异或操作, 得到的结果为 8bit 密文。

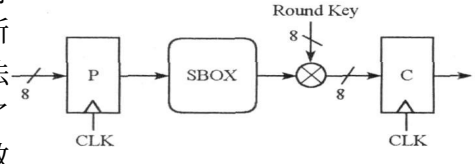

图7 DPA 攻击模型电路

Fig. 7 DPA attack model circuit

在实际的 AES 算法电路中, 128bit 的密文由 16 个上述电路并行执行产生, DPA 攻击者可以对每 8bit 密钥分别进行猜测攻击。因此, 利用图 7 所示的模型电路进行抗 DPA 攻击能力分析具有实际意义。

在模型电路的实现过程中, 我们首先采用全定制的方法设计了两输入的 LBDL 与、或、异或、同或、与非、或非逻辑门以及反向器, 并提取相应 LEF 视图建立了基于 LBDL 逻辑的单元库。然后采用第 2 节介绍的设计流程实现了模型电路的版图, 如图 8 所示。流程中逻辑综合工具采用的是 Synopsys 公司的 Design Compiler, 布局布线工具使用的是 Cadence 公司的 SOC Encounter, 网表替换以及连线的复制、平移操作采用自行编写的 PERL 脚本实现。

我们采用了与文献[8]中相同的方法对模型电路进行了 DPA 攻击模拟和电路抗 DPA 攻击性能分析。首先, 分别对模型电路进行了 2000 个随机输入的 SPICE 模拟, 并存储每次加密操作的输出密文和电路瞬态电流。所有的加密操作都使用 84 作为轮密钥。模拟采用的时钟频率为 50MHz, 每个时钟周期采样 400 个瞬态电流数据。然后, 利用取得的数据进行 DPA 攻击模拟: 选择 8bit 输入数据的第 3 位作为

攻击分析的目标函数,然后根据密文和穷举猜测的密钥反推对应的分析目标值,最后再根据分析目标的推测值对瞬态电流样本进行差分分析。为了对比模拟 DPA 攻击的效果,还采用传统半定制流程用 0.18μm 下的标准单元库设计实现了不带任何防护技术的模型电路。

图 9 所示为加密操作样本数为 2000 时的 DPA 攻击结果,横坐标为穷举猜测的 256 个密钥值。对于普通逻辑实现的模型电路,在正确的密钥猜测值(84)处,差分电流表现出了明显的尖峰,说明本文的模拟 DPA 攻击能够有效破解与功耗相关的密钥。而对于 LBDL 逻辑实现的模型电路,由于电路中所有信号的翻转率以及翻转时刻都不与输入信号取值相关,因此在 2000 个加密操作后,差分电流在密钥(84)处没有表现出明显的尖峰。

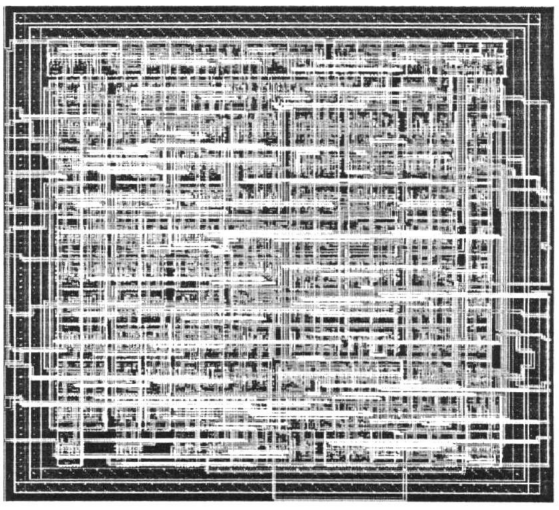

图 8 模型电路版图

Fig. 8 Layout of model circuit

我们采用成功实施 DPA 攻击所需的采样数量(MTD: Measurements to Disclosure)来评估模型电路的抗 DPA 攻击能力[12]。图 10 显示了随着加密操作次数的增加,各种密钥猜测值所对应的差分电流变化情况,其中黑色曲线对应正确密钥猜测值的分析结果,而其他曲线对应错误的密钥猜测值。从图中可以看出,对于普通逻辑实现的模型电路,DPA 攻击在大约 750 次加密采样后就可以破解出密钥;而 LBDL 逻辑实现的模型电路在 2000 个加密采样后,正确密钥对应的差分电流仍然没有表现出与其他密钥的差别。由此可见,采用本文所提出的基于 LBDL 逻辑的设计方法实现的电路具有有效的抗 DPA 攻击能力。

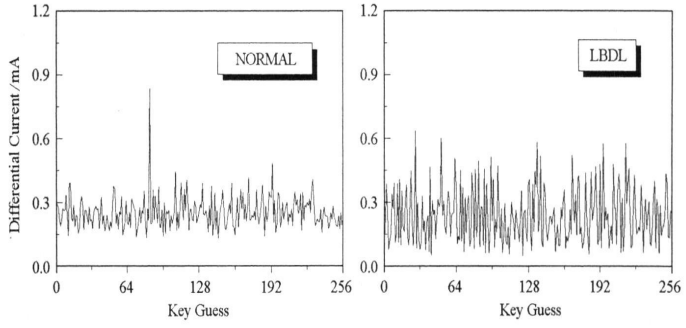

图 9 DPA 攻击结果

Fig. 9 Result of DPA attack

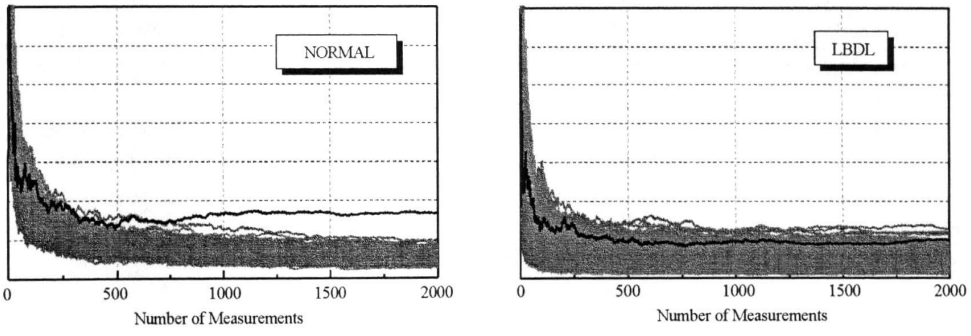

图 10 DPA 攻击的 MTD

Fig. 10 MTD of DPA attack

表 1 对 LBDL 逻辑和普通标准单元实现的模型电路进行了面积、延迟和功耗的对比。在面积方面, LBDL 逻辑的开销约为普通标准单元的 3 倍, 这是因为每个 LBDL 逻辑门需要由两个基本单元构成。在信号传输延时方面, 由于本文使用的 LBDL 逻辑单元种类较少, 难以进行有效的时序优化, 因此信号延时的开销接近于普通标准单元的 2 倍; 而且由于 LBDL 逻辑采用了动态工作模式, 在每个时钟周期, 数据吞吐率降低了一半。但如果能够建立比较完善的 LBDL 逻辑单元库, 且使用具有偏斜相位的时钟信号就能有效提高 LBDL 电路的延时性能。在功耗方面, LBDL 逻辑表现出了比普通逻辑更低的功耗, 一方面因为普通逻辑模拟时采用了更高的时钟频率, 而另一方面则是因为 LBDL 逻辑中不存在毛刺信号产生的功耗。

表 1 两种逻辑对比

Tab. 1 Compare of two logic styles

逻辑	面积		延时(ns)		功耗(mA)	
	高度(μm)	宽度(μm)	预充电	求值	平均	峰值
LBDL 逻辑	136	142	7.9	2.2	1.23	7.78
普通逻辑	80	80	4.2		1.36	11.81

4 总 结

本文提出了一种具有功耗恒定特性的动态差分逻辑 LBDL, 并介绍了基于 LBDL 逻辑的集成电路设计方法。相对于典型的抗 DPA 攻击逻辑 WDDL, LBDL 逻辑的优点在于其逻辑单元的信号翻转时刻与输入信号取值无关, 从而能够解决 WDDL 逻辑中存在的 DPA 攻击隐患。通过实践证明, 本文所提出的基于 LBDL 逻辑的电路设计方法能够很好地与现有的商用 EDA 设计工具结合, 具有良好的实用性。根据 SPICE 模拟分析, 由本文所提出的设计方法实现的电路具有有效的 DPA 防护效果。本文实现的模型电路在面积和性能上与普通逻辑相比存在一定的面积和性能开销, 通过建立较完善的 LBDL 逻辑单元库可以对其进行改进。

参 考 文 献:

[1] Kocher P, Jaffe J, Jun B. Differential Power Analysis[C]// CRYPTO, 1999: 388- 397.

[2] Tiri K, Akmal M, Verbauwhede I. A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards[C]// ESSCIRC, 2002: 403- 406.

[3] Tiri K, Verbauwhede I. A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation[C]// Design Automation and Test in Europe Conference and Exposition, 2004: 246- 251.

[4] Tiri K, Hwang D, Hodjat A, et al. Prototype IC with WDDL and Differential Routing DPA Resistance Assessment[C]// CHES, 2005: 354- 365.

[5] Mace F, Standaert F X, Hassoune I, et al. A Dynamic Current Mode Logic to Counteract Power Analysis Attacks[C]// DCIS, 2004: 186- 191.

[6] Bucci M, Giancane L, Luzzi R, et al. Three-phase Dual-rail Pre-charge Logic[C]// CHES, 2006: 232- 241.

[7] Popp T, Mangard S. Masked Dual-rail Pre-charge Logic: DPA-resistance without Routing Constraints[C]// CHES, 2005: 172- 186.

[8] Tiri K, Verbauwhede I. A VLSI Design Flow for Secure Side-channel Attack Resistant ICs[C]// Design Automation and Test in Europe Conference, 2005.

[9] Popp T, Kirschbaum M, Zefferer T, et al. Evaluation of the Masked Logic Style MDPL on a Prototype Chip[C]// CHES, 2007: 81- 94.

[10] Suzuki D, Saeki M. Security Evaluation of DPA Countermeasures Using Dual-rail Pre-charge Logic Style[C]// CHES, 2006: 255- 269.

[11] Tiri K, Verbauwhede I. Place and Route for Secure Standard Cell Design[C]// 6th International Conference on Smart Card Research and Advanced Applications, 2004: 143- 158.

[12] Tiri K, Verbauwhede I. Simulation Models for Side-channel Information Leaks[C]// DAC, 2005: 228- 233.