

基于差分传输管预充电逻辑的功耗恒定性电路改进设计

姚茂群* 李聪辉

(杭州师范大学信息科学与工程学院 杭州 311121)

摘 要: 通过分析差分传输管预充电逻辑(DP²L)的电路结构,发现该电路还无法达到完全的功耗恒定特性,仍然存在被功耗攻击的风险。针对该问题,该文对DP²L的电路结构进行改进,并用Hspice对改进前后的电路进行模拟仿真测试。实验表明:改进后的DP²L电路结构具有更好的功耗恒定特性,更能满足该逻辑电路的设计要求。

关键词: 功耗攻击; 功耗恒定; 双轨预充电逻辑; 差分传输管预充电逻辑

中图分类号: TN791

文献标识码: A

文章编号: 1009-5896(2021)07-1834-07

DOI: 10.11999/JEIT200513

Improved Design of Constant Power Consumption Circuit Based on Differential Pass-transistor Precharge Logic

YAO Maoqun LI Conghui

(School of Information Science and Engineering, Hangzhou Normal University, Hangzhou 311121, China)

Abstract: By analyzing the circuit structure of Differential Pass-transistor Precharge Logic (DP²L), it is found that the circuit can not achieve the complete constant power consumption, and there is still a risk of being attacked by power attack. To solve this problem, the circuit structure of DP²L is improved by this paper, and the circuits before and after the improvement are simulated using Hspice. The experimental results show that the improved DP²L circuit structure has better characteristics of constant power consumption and can better meet the design requirements of the logic circuit.

Key words: Power attack; Power consumption constant; Dual-Rail Precharge (DRP) logic; Differential Pass-transistor Precharge Logic (DP²L)

1 引言

功耗分析攻击是当前众多旁路攻击中一种有效且易于操作的攻击方法,其通过获取电子元器件在运行时所产生的功耗,并利用该功耗与元器件中所运行密码算法的某些运算结果之间的相关性来进行分析,进而获得有价值的秘密信息^[1-5]。而这一相关性是由当前流行的数字集成电路逻辑——CMOS逻辑单元所决定的,这种逻辑单元的功耗与其输入输出信号的翻转状态(“0→1”或“1→0”)有密切联系,并且这两种信号翻转时的电流所对应产生的电路功耗是不同的。而当CMOS逻辑单元在连续的两个时钟周期都没有发生信号的翻转时,由于没有产生动态电流,因此在这连续的时钟周期里电路所

产生的功耗较少,与有信号翻转时的电路功耗有明显的差异。因此,这种差异性就给攻击者通过分析功耗来获得秘密信息提供了理论依据^[6-11]。

近年来,研究者逐渐重视对电路级抗旁路攻击的研究,其中对功耗恒定性电路的研究是一个比较热门的方向。在这之中就有学者提出了一种可以让电路的功耗曲线不随信号取值变化而变化的双轨预充电逻辑结构(Dual Rail Precharge, DRP),其中最具代表性的是Tiri等人^[12]提出的SABL(Sense Amplifier Based Logic)电路和WDDL(Wave Dynamic Differential Logic)电路^[13]。因此也有众多学者基于这些逻辑电路做了相关的研究^[14-17],但是由于SABL, WDDL这些逻辑单元存在CMOS逻辑中固有的提前传播效应^[18],且电路中某一时刻的整体功耗是各个单元电路在这个时刻的叠加,因此跳变时间的不同就会造成整体功耗的差异。正是因为有了这种功耗差异,因此上述提到的DRP结构仍然存在被功耗攻击的风险。针对这些不足之处,国内有学者受到了互补传输管逻辑(Complementary Pass-transistor Logic, CPL)的启发,提出了一种

收稿日期: 2020-06-23; 改回日期: 2020-12-03; 网络出版: 2020-12-21

*通信作者: 姚茂群 yaomaoqun@163.com

基金项目: 国家自然科学基金(61771179), 浙江省自然科学基金(LY15F010011)

Foundation Items: The National Natural Science Foundation of China (61771179), Zhejiang Provincial Natural Science Foundation (LY15F010011)

基于 CPL 的新型双轨预充电逻辑——差分传输管预充电逻辑(Differential Pass-transistor Pre-charge Logic, DP²L)^[19], 该逻辑电路不仅可以实现功耗恒定的性质, 还可以消除以往DRP结构中存在的提前传播效应问题, 这极大地提升了电路在抗功耗攻击方面的能力。

但是, 利用Hspice软件进行仿真实验, 实验结果表明已提出的基于CPL结构的DP²L电路仍然存在一定程度的功耗信息泄露, 依旧存在被功耗攻击的可能性。对此, 本文在分析了该电路逻辑结构的基础之上, 对该电路的结构进行了改进, 使其更加满足功耗恒定的特性。并通过与改进前的电路进行比较, 验证了改进后电路在功耗恒定上的优势。

2 DP²L双轨预充电逻辑电路

CMOS逻辑单元在输出端信号发生“0→1”翻转或“1→0”翻转时消耗能量。除此之外, 电路不消耗能量。因此众多研究者基于这种相关性进行了较多的研究, 并已经提出了多种可以消除这种相关性的功耗恒定性电路逻辑, 例如SABL, WDDL, LBDL^[20]以及DP²L逻辑等等, 这些电路逻辑都属于不同结构的双轨预充电逻辑。

双轨预充电逻辑的特点如下:

(1) 一个双轨预充电逻辑电路是由两个单轨预充电逻辑电路组合而成的;

(2) 双轨(单轨)预充电逻辑电路的一个时钟周期分为预充电和求值两个阶段;

(3) 预充电阶段时, 双轨(单轨)预充电逻辑电路的所有互补输入信号端都输入预充电值低电平“0”。求值阶段时, 所有互补输入信号端都输入互补值;

(4) 预充电阶段时, 双轨(单轨)预充电逻辑电路的输出端都输出低电平“0”信号。求值阶段时, 双轨预充电逻辑门采用了差分互补的双端输出形式, 即若一个输出信号为高电平“1”, 则另一个输出信号必为低电平“0”。

这样设计的目的就是使得双轨预充电逻辑电路从预充电阶段进入求值阶段时, 不管输入信号取何互补值, 两个互补输出端都是仅有一个会发生“0→1”的翻转。当从求值阶段进入预充电阶段时, 互补输出端也是仅有一个发生“1→0”的翻转。这就保证了固定的信号翻转率和功耗恒定性, 消除了输入信号与功耗的相关性。

图1和图2分别为DP²L单轨和双轨输出“或”逻辑门, 通过这两个电路结构来详细阐述其预充电和求值过程。图1中P1~P6的6个PMOS管用来实现电路的预充电功能; NMOS管N5和N6用来实现

该电路的具体逻辑。即当输入端输入互补信号值时, 电路进入求值阶段, 此时这两个NMOS管中的一个会被导通, 从而形成一条从输入端到反相器的通路; 余下的NMOS管N1~N4的主要作用是消除提前传播效应^[19]; 反相器是作为输出负载的驱动单元。例如, 在预充电阶段, (a, b) 接收到输入信号 $(0, 0)$, $(\bar{a}, \bar{b})$ 也接收到输入信号 $(0, 0)$, 这时该逻辑单元的所有PMOS管都被导通, 电源 V_{DD} 经过反相器之后输出低电平“0”; 当进入求值阶段时, 若 (a, b) 接收到输入信号 $(1, 1)$, 则 $(\bar{a}, \bar{b})$ 接收到输入信号 $(0, 0)$, 此时N2, N4, N5分别打开, N1, N3, N6保持关闭状态, 此时就只有N2, N5和反相器构成一条唯一通路, 该条通路将连接N2的 $\bar{b}$ 信号值输送到反相器, 经过反相器后输出端 q 的值为高电平“1”, 满足“或门”的电路逻辑。

而其他逻辑功能单元只需要替换电路最左侧一列的两个输入信号就可以利用类似的电路结构来实现^[19]。

将单轨预充电逻辑结构的正逻辑与其对应的负逻辑相组合, 就形成了DP²L双轨预充电逻辑结构。图2以“或门”为例给出了DP²L双轨输出“或”逻辑的构成方式, 它由“或”和“或非”单轨预充电逻辑结构组合而成, 其中“或”逻辑门的输出端与DP²L双轨输出端 q 直接相连, “或非”逻辑门的

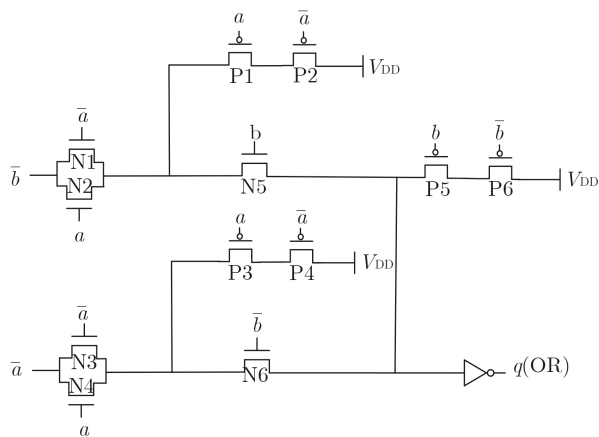


图1 DP²L单轨输出“或”逻辑

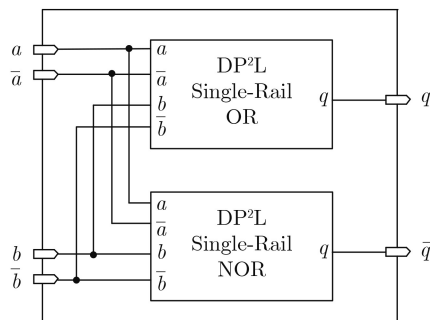


图2 DP²L双轨输出“或”逻辑的构成

输出端与DP²L双轨输出端 $\bar{q}$ 直接相连。因此,根据该电路的设计特点,若要实现DP²L双轨输出“或非”逻辑,则只需要将 q 和 $\bar{q}$ 交叉换线即可。该电路的具体工作步骤为:预充电阶段时,所有输入信号端都输入低电平预充电值“0”,根据之前对单轨逻辑的分析,这时双轨逻辑的输出端 q 和 $\bar{q}$ 的值也分别为“0”;求值阶段时,所有互补输入信号端均输入互补信号值,则双轨逻辑的输出端 q 和 $\bar{q}$ 也输出互补值。因此当电路从预充电阶段进入求值阶段后,不管输入信号端取何互补值,其两个输出端仅有一个会产生“0→1”的跳变,而另一个输出端的值则保持“0”不变;而当电路的求值阶段结束进入预充电阶段时,DP²L逻辑电路的输入信号端则都输入低电平预充电值“0”,此时逻辑电路的两个输出端中也仅有一个会产生“1→0”的跳变。

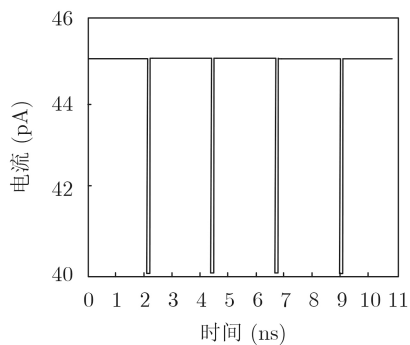
3 DP²L逻辑电路的功耗分析

通过对图1中DP²L单轨输出“或”逻辑的仔细分析,发现该电路逻辑在求值阶段晶体管充放电的数量并不相同。也就是说,电路功耗与输入信号的取值并不完全独立,仍然存在相关性。例如,当电路进入求值阶段,如果输入信号的值 $(a, \bar{a})$ 为(1, 0), $(b, \bar{b})$ 的值也为(1, 0),则NMOS管N2, N5导通, PMOS管P2, P6导通,由于P1, P5断开,则电路将仅对N2, N5两个晶体管放电。而当输入端信号的值

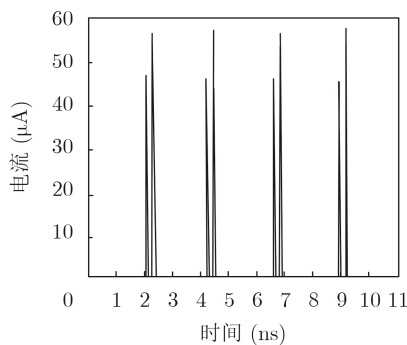
$(a, \bar{a})$ 为(0, 1), $(b, \bar{b})$ 的值也为(0, 1)时, NMOS管N3, N6导通, PMOS管P3, P5导通,电路将对这4个管子放电。这样当输入信号不同时,电路所消耗的功耗就会因为晶体管放电数目不同而造成差异,使得电路不能达到完全的功耗平衡。

为了验证此分析,利用Hspice软件对DP²L单轨输出“或”逻辑进行模拟实验,图3中有明显电流峰值的部分为电路进入求值阶段后输入信号 (a, b) 的值分别为(0, 0), (0, 1), (1, 0), (1, 1)时的电源端瞬态电流曲线,即可以表示为运行时的逻辑电路功耗变化。图中横坐标表示运行时间,纵坐标表示电源端瞬态电流,将相同的输入信号运行4个周期以保证数据的准确性。图中以2.3 ns为一个周期,一个周期中包含预充电和求值两个阶段,其中有明显电流峰值的时段为求值阶段,其余皆为预充电阶段。图中可看出一个周期中包含两个相邻的电流峰值,先产生的电流峰值表示输出信号发生“0→1”翻转时产生的电流,后产生的电流峰值表示输出信号发生“1→0”翻转时产生的电流。

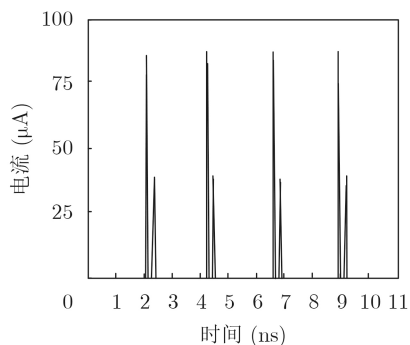
图3(a)由于输入信号 (a, b) 的值为(0,0)时,“或”逻辑输出并没有发生翻转,因此产生的动态功耗即电源端电流非常小;而输入其他信号时,由于发生了输出信号的翻转,即产生了充放电过程。并且可明显看出同一周期中电流曲线的相邻两个峰值具有明显差异,这个差异是由输出信号发生“0→1”,



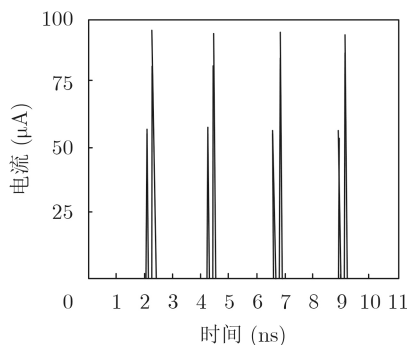
(a) 输入信号 $a=0, b=0$ 时的瞬态电流曲线



(b) 输入信号 $a=0, b=1$ 时的瞬态电流曲线



(c) 输入信号 $a=1, b=0$ 时的瞬态电流曲线



(d) 输入信号 $a=1, b=1$ 时的瞬态电流曲线

图3 4种输入信号下的DP²L单轨输出“或”逻辑瞬态电流曲线

“1→0”翻转时所产生的不同功耗所造成的。因此,攻击者仍然可以利用这个差异进行有效的攻击。

4 DP²L逻辑电路的改进

经过以上对DP²L逻辑的分析,图4所示为改进后的DP²L单轨输出“或”逻辑。分析如下:在求值阶段时,当输入端($a, \bar{a}$)的值为(1, 0), ($b, \bar{b}$)的值也为(1, 0)时, NMOS管N2, N5导通, PMOS管P3, P11导通, 则电路将仅对N2, N5, P3, P11这4个晶体管放电。而当输入端信号($a, \bar{a}$)的值为(0, 1), ($b, \bar{b}$)的值也为(0, 1)时, NMOS管N3, N6导通, PMOS管P5, P9导通, 则电路也将对4个管子放电。因此,在求值阶段不管输入信号为何值,晶体管的翻转数量都是恒定的;而预充电阶段时,输入信号都为低电平“0”,此时由于PMOS管全部都被导通,因此晶体管的放电数量亦恒定。因此只要保证逻辑电路中所使用的PMOS管的规格参数全部相同, NMOS管的规格参数也全部相同,则经过改进后的DP²L逻辑在不同阶段的功耗都是由相同参数和数量的晶体管充放电产生的,这就保证了功耗恒定的性质。其他的基于DP²L的逻辑门电路根据相同的改进方法即可达到相同的效果。

为了验证此分析,通过Hspice软件对改进后的DP²L单轨输出“或”逻辑进行模拟,图5中有明显电流峰值的部分为求值阶段时输入信号(a, b)的值分别为(0, 0), (0, 1), (1, 0), (1, 1)时的电源端电流

曲线。所使用的模拟实验方法与图3中所使用的完全相同。

由以上模拟结果可知,经过改进后的DP²L单轨输出“或”逻辑在不同输入信号取值的情况下,一个周期中相邻两个电流峰值的差异较小,与改进前相比有较大的改善。这就保证了电路在输出信号发生“0→1”, “1→0”翻转时具有近乎相等的功耗,从而改善了功耗恒定的特性。

将改进后的DP²L单轨输出“或”逻辑和改进后的DP²L单轨输出“或非”逻辑相组合就构成了如图2所示的DP²L双轨输出“或”逻辑。利用

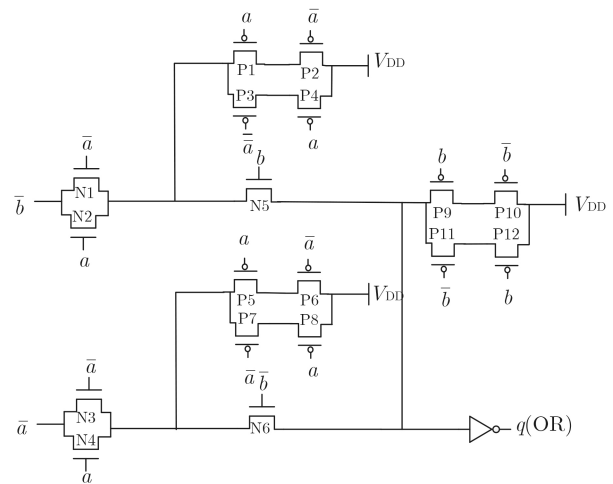


图4 改进后DP²L单轨输出“或”逻辑

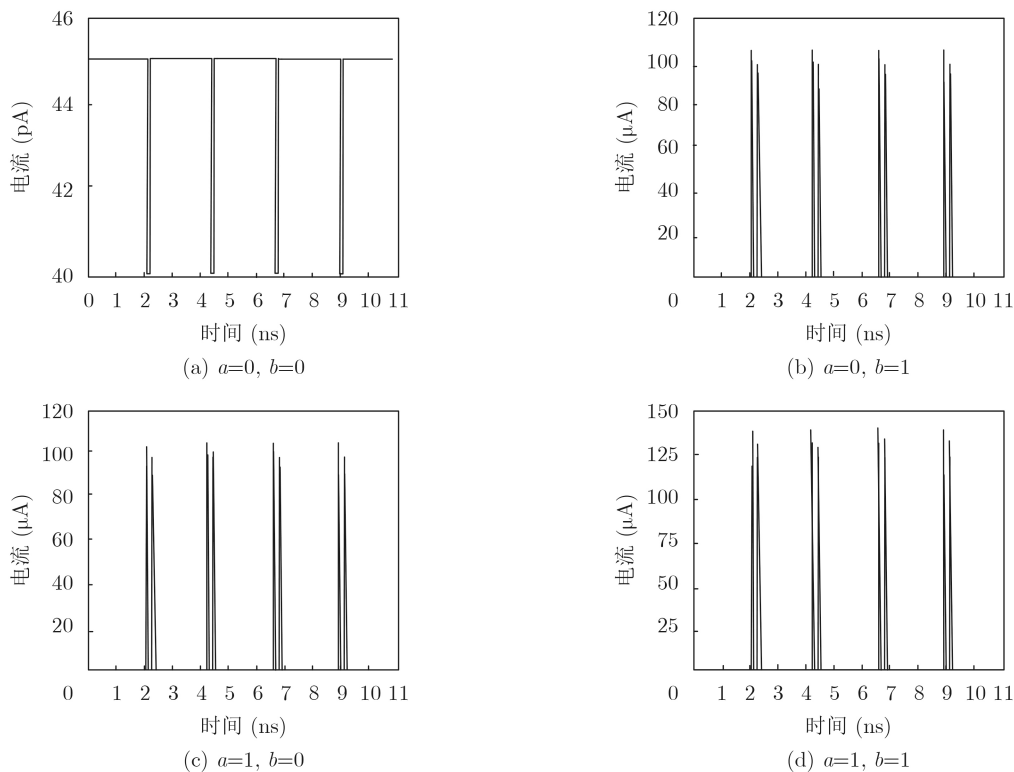


图5 4种输入信号下的改进后DP²L单轨输出“或”逻辑瞬态电流曲线

Hspice对该DP²L双轨输出“或”逻辑进行模拟,图6中有明显电流峰值的部分为求值阶段时输入信号(a, b)的值分别为(0, 0), (0, 1), (1, 0), (1, 1)时的电源端电流曲线。所使用的模拟实验方法与图3中

所使用的完全相同。分析可得:不管输入端的信号取何值,该逻辑门电路所表现出的功耗都是完全恒定的,并且当输出信号产生“0→1”和“1→0”翻转时电路所产生的功耗也是近似相同的。

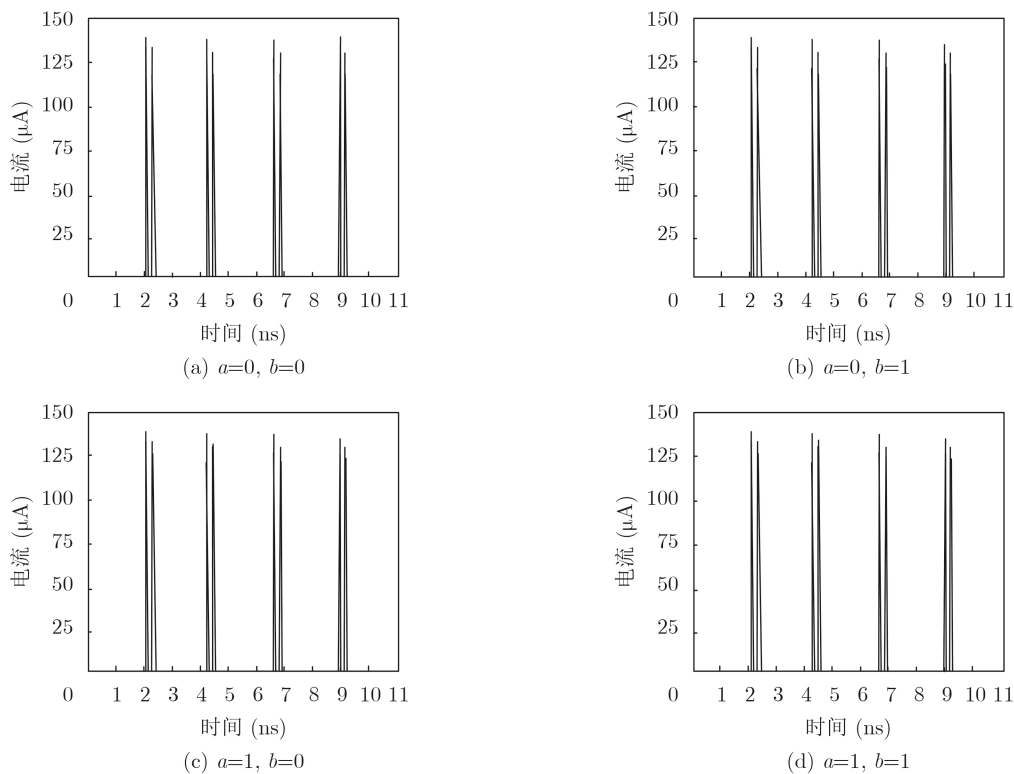


图6 4种输入信号下改进后DP²L双轨输出“或”逻辑瞬态电流曲线

5 功耗恒定性分析

为验证改进后DP²L电路的功耗恒定特性,将图3、图5、图6中的数据进行分析和整理,如表1—

表1 改进前DP²L单轨电路相关参数

输入条件	$a=0, b=0$	$a=0, b=1$	$a=1, b=0$	$a=1, b=1$
“0→1”翻转电流(μA)	/	48.86	87.82	62.12
“1→0”翻转电流(μA)	/	58.17	38.75	97.74
NED(%)	33.05			

表2 改进后DP²L单轨电路相关参数

输入条件	$a=0, b=0$	$a=0, b=1$	$a=1, b=0$	$a=1, b=1$
“0→1”翻转电流(μA)	/	108.32	107.65	140.18
“1→0”翻转电流(μA)	/	97.96	98.31	136.58
NED(%)	25.58			

表3所示,表4为国际上同类型逻辑电路的功耗恒定性比较。表中分别列出了电路改进前后在不同输入条件下发生“0→1”和“1→0”翻转时电流数据的平均值,以及衡量功耗恒定特性的评价指标:标准化能量偏差(Normalized Energy Deviation, NED)^[13]。其定义为

$$\text{NED} = \frac{\max(E) - \min(E)}{\max(E)}$$

式中, E 是电路在一个运算周期所产生的功耗值的

表3 改进后DP²L双轨电路相关参数

输入条件	$a=0, b=0$	$a=0, b=1$	$a=1, b=0$	$a=1, b=1$
“0→1”翻转电流(μA)	139.12	139.01	139.67	139.51
“1→0”翻转电流(μA)	136.73	136.51	136.95	136.82
NED(%)	0.40			

表4 同类型逻辑实现的“或”门标准化能量偏差对比

逻辑电路	WDDL	改进前DP ² L双轨电路	LBDL	改进后DP ² L双轨电路
NED(%)	11.50	5.36	3.23	0.40

集合。NED的取值范围在[0,1], 且数值越小表明该电路的功耗恒性能越好。

由表4可得, 改进后的DP²L电路在功耗恒定特性上明显优于其他逻辑电路, 前者较高的NED值就表现出了一定程度的数据与功耗的相关性, 更容易遭受到功耗攻击。而改进后的电路以其较低的NED值就体现出了较高的抗功耗攻击性能。

6 结束语

通过分析DP²L电路的功耗恒定特性并经过Hspice软件的模拟验证, 发现该电路无法完全满足功耗恒定特性。因此本文对DP²L电路进行改进, 并对改进后电路进行仿真测试和NED值的比较, 结果表明改进后的DP²L电路在功耗恒定的特性上有了明显的提升, 从而进一步为密码功能模块的可靠性和安全性提供有力支撑。

参 考 文 献

- [1] 黄海, 冯新新, 刘红雨, 等. 基于随机加法链的高级加密标准抗侧信道攻击对策[J]. 电子与信息学报, 2019, 41(2): 348–354. doi: [10.11999/JEIT171211](#).
- [2] 陈华, 刁伟, 范丽敏, 等. 密码产品的侧信道分析与评估[J]. 电子与信息学报, 2020, 42(8): 1836–1845. doi: [10.11999/JEIT190853](#).
- [3] CHEN Hua, XI Wei, FAN Limin, *et al.* Side channel analysis and evaluation on cryptographic products[J]. *Journal of Electronics & Information Technology*, 2020, 42(8): 1836–1845. doi: [10.11999/JEIT190853](#).
- [4] UTYAMISHEV D and PARTIN-VAISBAND I. Real-time detection of power analysis attacks by machine learning of power supply variations on-chip[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2020, 39(1): 45–55. doi: [10.1109/TCAD.2018.2883971](#).
- [5] ASHOK P and VETTUVANAM SOMASUNDARAM K B. Charge balancing symmetric pre-resolve adiabatic logic against power analysis attacks[J]. *IET Information Security*, 2019, 13(6): 692–702. doi: [10.1049/iet-ifs.2018.5136](#).
- [6] MESSERGES T S, DABBISH E A, and SLOAN R H. Examining smart-card security under the threat of power analysis attacks[J]. *IEEE Transactions on Computers*, 2002, 51(5): 541–552. doi: [10.1109/TC.2002.1004593](#).
- [7] SENGUPTA A, MAZUMDAR B, YASIN M, *et al.* Logic locking with provable security against power analysis attacks[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2020, 39(4): 766–778. doi: [10.1109/TCAD.2019.2897699](#).
- [8] GOHIL N N and VEMURI R R. Automated synthesis of differential power attack resistant integrated circuits[C]. 2019 IEEE National Aerospace and Electronics Conference, Dayton, USA, 2019: 204–211. doi: [10.1109/NAECON.46414.2019.9057882](#).
- [9] ZHENG Zhen and YAN Yingjian. Design of a power randomization circuit for block ciphers[C]. The IEEE 4th International Conference on Integrated Circuits and Microsystems, Beijing, China, 2019: 6–11. doi: [10.1109/ICICM48536.2019.8977152](#).
- [10] KUMAR S D and THAPLIYAL H. Exploration of non-volatile MTJ/CMOS circuits for DPA-resistant embedded hardware[J]. *IEEE Transactions on Magnetics*, 2019, 55(12): 3401308. doi: [10.1109/TMAG.2019.2943053](#).
- [11] HWANG D D, TIRI K, HODJAT A, *et al.* AES-based security coprocessor IC in 0.18- μm CMOS with resistance to differential power analysis side-channel attacks[J]. *IEEE Journal of Solid-State Circuits*, 2006, 41(4): 781–792. doi: [10.1109/JSSC.2006.870913](#).
- [12] AVITAL M, LEVI I, KEREN O, *et al.* CMOS based gates for blurring power information[J]. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2016, 63(7): 1033–1042. doi: [10.1109/TCSI.2016.2546387](#).
- [13] 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[C]. The 28th European Solid-state Circuits Conference, Florence, Italy, 2002: 403–406.
- [14] TIRI K and VERBAUWHEDE I. A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation[C]. The Design, Automation and Test in Europe Conference and Exhibition, Paris, France, 2004: 246–251. doi: [10.1109/DATE.2004.1268856](#).
- [15] 钱浩宇, 汪鹏君, 丁代鲁, 等. 基于SABL的防御差分功耗分析移位寄存器设计[J]. 电子技术应用, 2017, 43(2): 40–43. doi: [10.16157/j.issn.0258-7998.2017.02.008](#).
- [16] QIAN Haoyu, WANG Pengjun, DING Dailu, *et al.* Design of resistant differential power analysis shift register based on SABL[J]. *Application of Electronic Technique*, 2017, 43(2): 40–43. doi: [10.16157/j.issn.0258-7998.2017.02.008](#).
- [17] BUCCI M, GIANCANE L, LUZZI R, *et al.* A flip-flop for the DPA resistant three-phase dual-rail pre-charge logic family[J]. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2012, 20(11): 2128–2132. doi: [10.1109/tvlsi.2011.2165862](#).
- [18] YU Weize and WEN Yiming. Leveraging balanced logic gates as strong PUFs for securing IoT against malicious

- attacks[J]. *Journal of Electronic Testing*, 2019, 35(6): 853–865. doi: [10.1007/s10836-019-05833-9](https://doi.org/10.1007/s10836-019-05833-9).
- [17] BELLIZIA D, SCOTTI G, and TRIFILETTI A. TEL logic style as a countermeasure against side-channel attacks: Secure cells library in 65nm CMOS and experimental results[J]. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2018, 65(11): 3874–3884. doi: [10.1109/TCSI.2018.2861738](https://doi.org/10.1109/TCSI.2018.2861738).
- [18] 乐大珩. 抗功耗攻击的密码芯片电路级防护关键技术研究[D]. [博士论文], 国防科学技术大学, 2011.
- YUE Daheng. Research on circuit-level design against power analysis attack for cryptographic chip[D]. [Ph. D. dissertation], National University of Defense Technology, 2011.
- [19] 王晨旭. 密码芯片抗功耗攻击技术研究[D]. [博士论文], 哈尔滨工业大学, 2013.
- WANG Chenxu. Research on the power analysis resistant technology of cryptographic IC[D]. [Ph. D. dissertation], Harbin Institute of Technology, 2013.
- [20] 乐大珩, 李少青, 张民选. 基于LBDL逻辑的抗DPA攻击电路设计方法[J]. 国防科技大学学报, 2009, 31(6): 18–24. doi: [10.3969/j.issn.1001-2486.2009.06.004](https://doi.org/10.3969/j.issn.1001-2486.2009.06.004).
- YUE Daheng, LI Shaoqing, and ZHANG Minxuan. An LBDL based VLSI design method to counteract DPA attacks[J]. *Journal of National University of Defense Technology*, 2009, 31(6): 18–24. doi: [10.3969/j.issn.1001-2486.2009.06.004](https://doi.org/10.3969/j.issn.1001-2486.2009.06.004).
- 姚茂群: 女, 1967年生, 教授, 研究方向为低功耗数字集成电路设计、智能控制、神经网络和模糊逻辑、物联网及应用.
- 李聪辉: 男, 1996年生, 硕士生, 研究方向为低功耗数字集成电路设计、硬件安全.

责任编辑: 马秀强