文章编号：2095-4980(2024)12-1421-05

基于掩码技术的抗功耗攻击电路方案设计

李聪辉[1]，姚茂群*[2]

(1.台州科技职业学院 信息工程学院，浙江 台州 318020；2.杭州师范大学 信息科学与技术学院，浙江 杭州 311121)

摘　要：掩码技术所具有的混淆特性可加大攻击者对电路逻辑值的分析难度，与双轨预充电技术相结合可进一步起到抗功耗攻击的作用。掩码技术和双轨预充电技术的采用需要对电路的输入和输出信号进行相应的处理。据此，本文提出了单-双轨转换逻辑电路，可实现单轨信号和双轨信号的相互转换。之后提出了掩码转换逻辑电路，可实现电路的输出值根据掩码值转换。最后进一步提出了单-双轨掩码逻辑结构，形成一个具有抗功耗攻击性能的电路设计方案。以上逻辑电路经过了Hspice仿真验证，具有正确的逻辑功能，为抗功耗攻击电路的设计提供了一种思路。

关键词：密码芯片；功耗攻击；掩码技术；逻辑混淆；双轨预充电技术

中图分类号：TN791　　**文献标志码：**A　　**doi：**10.11805/TKYDA2023070

Design of circuit against power analysis attacks based on masking technology

LI Conghui[1]，YAO Maoqun*[2]

(1.School of Information Engineering，Taizhou Vocational College of Science and Technology，Taizhou Zhejiang 318020，China；
2.School of Information Science and Technology，Hangzhou Normal University，Hangzhou Zhejiang 311121，China)

Abstract：The confusion characteristic of masking technology can increase the difficulty of attackers to analyze the logic value of the circuit，and the combination of masking technology and Dual-Rail Precharge(DRP) technology can further play a role in resisting power analysis attacks. The application of masking technology and dual-rail precharge technology requires corresponding processing of the input signals and output signals. Based on this，this paper proposes a single rail to dual-rail conversion logic circuit，which can realize the conversion of signal. Then a mask logic conversion circuit is proposed，which can realize the conversion of the output value of the circuit according to the mask value. At last，a single-dual rail mask logic structure is proposed to form a circuit design scheme with power attack resistance. The above logic circuits have been verified by Hspice simulation and have correct logic functions，which provides a way for the circuit design against power analysis attacks.

Keywords：crypto chip；power analysis attacks；masking technology；logic obfuscation；Dual-Rail Precharge(DRP) technology

功耗攻击是一种针对硬件电路的攻击方式，攻击目标通常为密码芯片，其主要通过分析电路在处理不同数据时所表现出的功耗差异来建立模型并进行统计学上的分析，以得出功耗与数据之间的相关性。这种相关性可以让攻击者获得所需要的秘密数据，以完成攻击任务。基于这种攻击原理，国内外有众多专家学者提出了一些切实可行的抗功耗攻击的方法，主要可以分为算法级和电路级。算法级的抗功耗攻击方法主要是对密码算法进行设计，相当于推出一种新型的密码算法来加强密码芯片的安全性[1-3]。电路级的抗功耗攻击方法主要通过重新设计底层的硬件电路单元，并将其运用到密码芯片中的关键逻辑之中[4-5]。电路级的方法主要可以分为功耗恒定化和功耗随机化，这两种方法的核心都在于将电路所处理数据与功耗进行无关化处理。具体来说，功耗恒定化就是当电路逻辑单元处理数据时功耗保持恒定，而功耗随机化就是当电路逻辑单元处理数据时功耗出现随机无

收稿日期：2023-03-23；**修回日期：**2023-07-13

基金项目：台州市科技计划资助项目(24gyb29)；国家自然科学基金资助项目(61771179)；台州科技职业学院2023年度校级课题资助项目(23QNZ09)

*通信作者：姚茂群　email:yaomaoqun@163.com

规律的改变。

掩码是一种可以起到逻辑混淆的技术，进而对逻辑信号进行隐藏，在算法级和电路级都有应用[6-7]。在算法级中，主要是在密码算法中引入随机掩码对算法中间值进行隐藏。在电路级中，主要是在电路的输入信号中增加掩码信号从而对电路输出值进行隐藏，据此已提出掩码型差分传输管预充电逻辑(Masked Differential Pass-transistor Precharge Logic，MDP2L)[8]。在已提出的MDP2L电路中，只涉及了基础门逻辑单元的设计，实现了门逻辑单元的功能。但是未提出该类型电路所需的单-双轨输入输出信号的相互转换电路，以及对经过隐藏的电路输出值进行恢复的设计方法，缺乏一个系统性的设计框架。据此，本文提出一种基于掩码技术的抗功耗攻击电路设计方案。

1 抗功耗攻击电路

1.1 双轨预充电技术

双轨预充电技术(DRP)[5,9,10]常用于设计功耗恒定化逻辑电路当中，该类型电路的工作过程可以分为预充电(Prch)和求值(Eval)2个阶段。一个双轨电路由2个单轨电路组成，这2个单轨电路在输出时的信号与整个电路所处的工作阶段有关。在预充电阶段，该逻辑电路的所有输入信号均置为低电平“0”，此时经过逻辑电路的运算，两个单轨电路的输出信号也均为“0”。而当处于求值阶段时，两个单轨电路在完成逻辑运算之后输出2个互补的信号。整个电路的运行过程可由图1来表示，具体运行原理为：当电路处于预充电阶段时，2个输出信号的值均为“0”。而当电路从预充电转为求值阶段时，无论输入信号为何值，2个输出信号中都有且仅有一个会形成“0→1”的翻转。同理，当电路从求值转为预充电阶段时，也只有一个输出信号会形成“1→0”的翻转，从而满足恒定的信号翻转率，进而达到功耗恒定的要求。

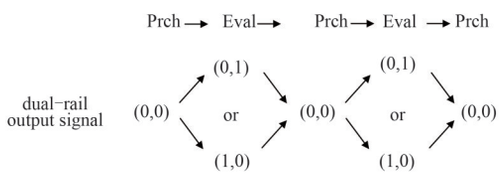

Fig.1 Dual-Rail Precharge process
图1 双轨预充电过程

1.2 MDP2L 逻辑电路

现已设计出多种MDP2L门逻辑电路，该逻辑门的输出值由掩码值m决定，即掩码值不同，整个逻辑门的输出值就会存在差异。这种差异性是攻击者难以获取的，再结合双轨预充电技术，可以让攻击者难以获得功耗与电路运算值之间的相关性，进而起到抗功耗攻击的作用。以图2所示的MDP2L单轨或逻辑门为例，具体来说：当处于求值阶段时，A1和A2区域负责电路的求值运算，当m=0时，由掩码信号控制的N型金属-氧化物-半导体(N-Metal-Oxide-Semiconductor，NMOS)管N7被导通，整个电路的运算由A1区域完成，此时电路输出值为或逻辑门的正逻辑；而当m=1时，NMOS管N14被导通，整个电路的运算由A2区域完成，此时电路输出值为或逻辑门的负逻辑；A3区域为整个逻辑电路的预充电部分，当处于预充电阶段时，由于输入信号均置为0，此时逻辑电路的输出值也为0。图3所示是MDP2L双轨或逻辑门[8]，其由MDP2L单轨或逻辑门和MDP2L单轨或非逻辑门组成。当电路处于预充电阶段时输出信号q和$\bar{q}$的值均为0，而当电路处于求值阶段时输出信号q和$\bar{q}$的值为互补关系。这就使得电路从预充电阶段转为求值阶段时，输出信号q和$\bar{q}$中只有一个信号会形成“0→1”的翻转，满足恒定的信号翻转

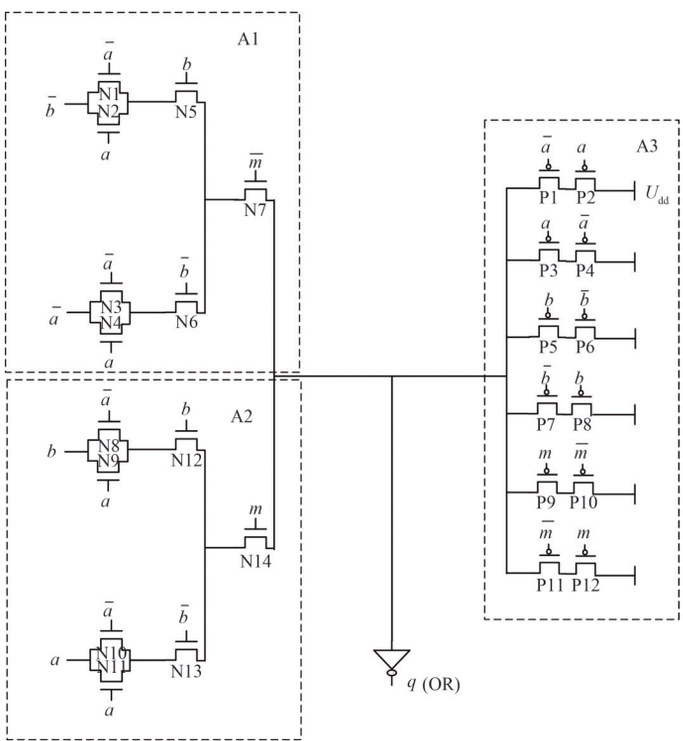

Fig.2 MDP2L single-rail OR gate
图2 MDP2L单轨或逻辑门

率。根据实验结果，该类型电路具有较好的功耗恒定特性。

2　单–双轨转换逻辑电路

根据利用双轨预充电技术所提出的MDP2L逻辑门可知，在预充电阶段和求值阶段，逻辑门对于输入信号的要求是不相同的。当逻辑门处于预充电阶段时，需要将所有的输入信号都置0，而当逻辑门处于求值阶段时，每个输入信号都要有与之互补的信号作为补充，进而形成一对互补信号。同理，当逻辑门输出时，需要将2个输出信号进行处理，“合并”为一个信号用于下一环节电路的输入。

据此，本文提出单–双轨转换逻辑电路，该逻辑电路由或非门和反相器组成，如图4所示。图4(a)为单轨转双轨逻辑(Single to Dual–Rail Logic，SDR Logic)电路，A为单轨输入信号，en作为区分预充电阶段和求值阶段的使能信号，a和$\bar{a}$为双轨输出信号。具体来说：当en=0时，说明后续双轨逻辑门需要处于预充电阶段，此时无论A信号是0还是1，输出信号a和$\bar{a}$的值均为0。而当en=1时，说明后续双轨逻辑门需要处于求值阶段，此时输出信号a的值应与A信号的值相同，并与$\bar{a}$的值相反，从而形成一对互补信号并作为后续电路的输入。图4(b)为双轨转单轨逻辑(Dual to Single Rail Logic，DSR Logic)电路，q和$\bar{q}$为该电路的输入，同时也是上一级双轨逻辑门的输出信号，Q为该电路的输出信号。具体来说：当接收到来自上一级的双轨输出信号q和$\bar{q}$并作为其输入信号之后，经过2个或非门的处理，可以使得Q=q，实现双轨信号到单轨信号的转换。其中，由于q和$\bar{q}$的值来自于上一级的双轨电路，则q和$\bar{q}$无论是在预充电阶段还是求值阶段都不会存在同时为1的情况。

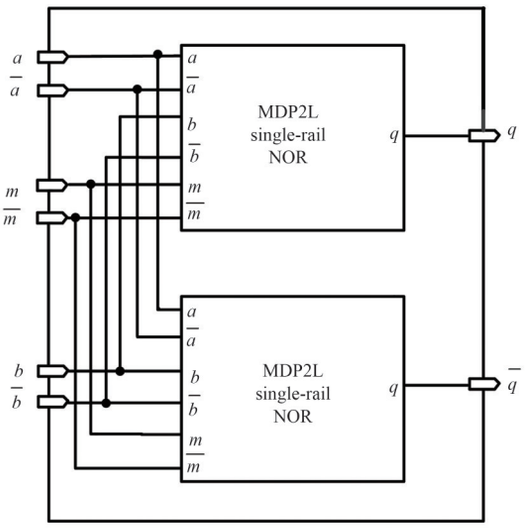

Fig.3 MDP2L dual–rail OR gate
图3 MDP2L双轨或逻辑门

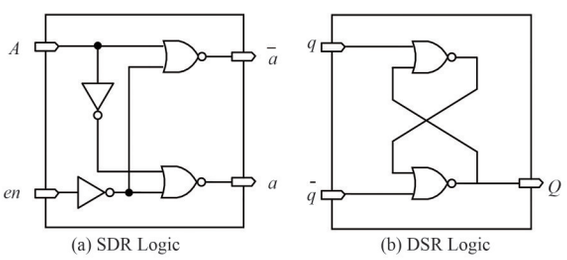

Fig.4 Single–dual rail conversion logic circuit
图4 单–双轨转换逻辑电路

表1 单轨转双轨逻辑电路真值表

Table1 Truth table of single to dual rail logic circuit

en	A	a	$\bar{a}$
0	0	0	0
0	1	0	0
1	0	0	1
1	1	1	0

表2 双轨转单轨逻辑电路真值表

Table2 Truth table of dual to single rail logic circuit

q	$\bar{q}$	Q
0	0	0
0	1	0
1	0	1

单轨转双轨逻辑电路和双轨转单轨逻辑电路的真值表分别如表1和表2所示。

3　掩码转换逻辑电路

在电路中引入掩码技术可以让密码芯片中关键部位逻辑单元的输出信号值产生随机性，从而混淆攻击者的分析，但若后续不对随机性的输出信号进行处理，将不可避免地造成信号的混乱。因此本文基于掩码技术，提出一种掩码转换逻辑(Mask Conversion Logic，MC Logic)电路，如图5所示。该电路由输入信号m、Q，输出信号Out，MOS管P1、N1和反相器组成。由MDP2L双轨或逻辑门的运行原理可知：当m=0时，MDP2L逻辑门输出或门的正逻辑。而当m=1时，该逻辑门输出或门的负逻辑。因此，后续的电路必须要根据掩码信号m的取值对MDP2L

表3 掩码转换逻辑电路真值表

Table3 Truth table of mask conversion logic circuit

m	Q	Out
0	0	0
0	1	1
1	0	1
1	1	0

类型逻辑门的输出信号进行处理，以实现正确的运算逻辑。据此，该掩码转换逻辑电路的运行原理为：当 m=0 时，由于上一级电路输出值为正逻辑，因此无需处理直接对电路信号进行输出；而当 m=1 时，由于上一级电路输出值为负逻辑，因此需要对电路信号进行反相处理。其中，m 作为掩码信号控制 MOS 管的导通状态。该电路真值表如表 3 所示。

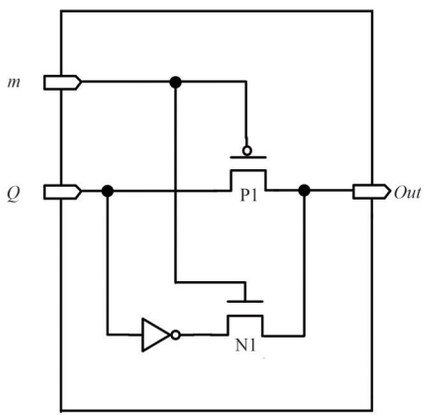

Fig.5 Mask conversion logic circuit
图 5 掩码转换逻辑电路

4 单–双轨掩码逻辑结构

为了在密码芯片的关键部件中实现一个基于掩码技术的抗功耗攻击逻辑电路，本文接着提出一种通用的单–双轨掩码逻辑(Single–Dual Rail Mask Logic，SDRM Logic)结构设计方案，如图 6 所示。该结构由如下电路模块组成：单轨转双轨逻辑(SDR Logic)电路、掩码生成逻辑(Mask Generation Logic，MG Logic)电路、掩码型双轨预充电逻辑(Masked Dual–Rail Precharge Logic, MDRP Logic)电路、双轨转单轨逻辑(DSR Logic)电路和掩码转换逻辑(MC Logic)电路。其中，MDRP 逻辑电路指的是使用了掩码和双轨预充电技术的逻辑电路，是整个逻辑结构的核心部 分，起到功耗恒定和混淆逻辑的作用，如 MDP2L 电路等。该逻辑结构的运行过程如下：a) 当有输入信号 Input 进入时，会通过单轨转双轨逻辑电路，将单轨信号转换为双轨信号，并作为下一模块的输入；b) 掩码生成电路负责随机信号掩码 m 的生成，并将其作为后续 2 个模块的输入；c) MDRP 逻辑电路接收到上一级电路模块的双轨信号和掩码信号之后，进行逻辑运算并输出双轨信号，并作为下一模块的输入；d) 双轨转单轨逻辑电路负责将上一级中输出的双轨信号转换回单轨信号，并作为下一模块的输入；e) 掩码转换逻辑电路根据掩码生成电路中掩码信号的取值将上一级的输出信号进行处理，进而使整个逻辑结构满足正确的逻辑输出。

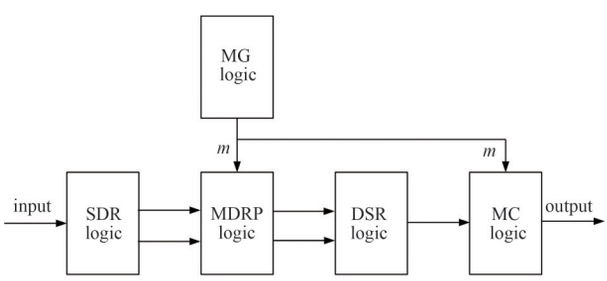

Fig.6 Single–dual rail mask logic structure
图 6 单–双轨掩码逻辑结构

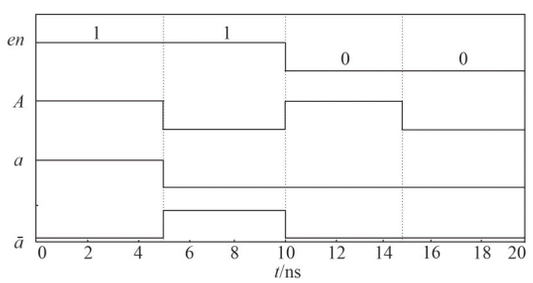

Fig.7 Signal waveforms of single to dual rail logic circuit
图 7 单轨转双轨逻辑电路信号波形

5 仿真结果

采用 Hspice 仿真软件，对所设计的逻辑电路进行功能测试。首先是如图 4(a)所示的单轨转双轨逻辑电路，采用高低电平的方式进行表示，其中 1 表示高电平，0 表示低电平，结果如图 7 所示。由图可得，当 en 为高电平时，电路处于求值阶段，a 信号的值与 A 相同，与 $\bar{a}$ 相反；而当 en 为低电平时，电路处于预充电阶段，输出信号 a 与 $\bar{a}$ 均为低电平，满足设计要求。

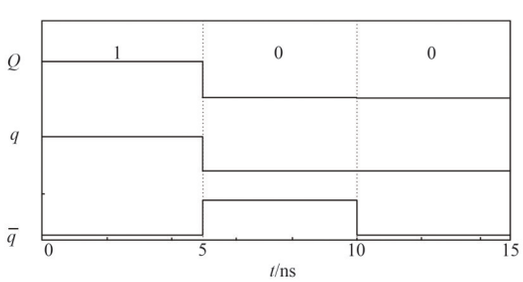

Fig.8 Signal waveforms of dual to single rail logic circuit
图 8 双轨转单轨逻辑电路信号波形

之后，对如图 4(b)所示的双轨转单轨逻辑电路进行相同的测试，结果如图 8 所示。由图可知，当 q 和 $\bar{q}$ 为互补信号时，表明此时为求值阶段，满足 Q=q 的逻辑关系。而当 q 和 $\bar{q}$ 的值均为 0 时，表明此时为预充电阶段，依然满足 Q=q。而根据双轨预充电技术的设计原理，不可能存在输入信号 q 和 $\bar{q}$ 的值均为 1 的情况，因此不予以模拟。

最后，对如图 5 所示的掩码转换逻辑电路进行相同的测试，结果如图 9 所示。由图可知，当 m=1 时，表明此

时需要对信号 Q 进行转换，即实现 Q 与 Out 的逻辑值相反。而当 m=0 时，表明此时无需对信号 Q 进行转换，即实现 Q 与 Out 的逻辑值相同。

6　结论

基于掩码技术的抗功耗攻击电路需要考虑掩码信号的取值对整个电路输出信号的影响，本文据此提出了掩码转换逻辑电路，实现对输出信号的处理。根据双轨预充电技术的运行原理，提出了单-双轨转换逻辑电路，实现单轨信号和双轨信号的相互转换。最后，将以上所设计的电路与MDRP类型逻辑电路相结合，提出了单-双轨掩码逻辑结构设计方案，并经过了仿真验证。

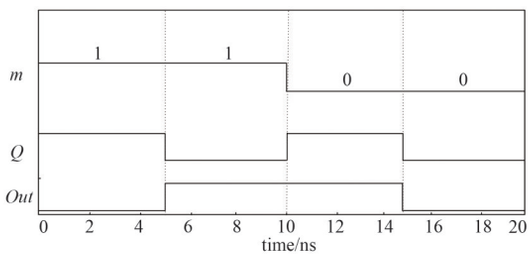

Fig.9 Signal waveforms of mask conversion logic circuit
图 9　掩码转换逻辑电路信号波形

参考文献：

[1] 王永娟,王涛,袁庆军, 等. 密码算法旁路立方攻击改进与应用[J]. 电子与信息学报, 2020,42(5):1087-1093. (WANG Yongjuan, WANG Tao, YUAN Qingjun, et al. Side channel cube attack improvement and application to cryptographic algorithm[J]. Journal of Electronics & Information Technology, 2020,42(5):1087-1093.) doi:10.11999/JEIT181075.

[2] 甘罕. 基于密码芯片的旁路攻击方法研究[D]. 北京:北京邮电大学, 2020. (GAN Han. Research on side channel attack method based on cryptographic chip[D]. Beijing,China:Beijing University of Posts and Telecommunications, 2020.)

[3] YAO Maoqun, LI Conghui, XUE Ziwei. Design of double-masking current-mode CMOS circuit against power analysis attacks[C]// 2021 IEEE 15th International Conference on Electronic Measurement & Instruments(ICEMI). Nanjing,China:IEEE, 2021: 285-288. doi:10.1109/ICEMI52946.2021.9679628.

[4] 李浪,欧雨,邹祎. 一种AES随机变换掩码方案及抗DPA分析[J]. 密码学报, 2018,5(4):442-454. (LI Lang,OU Yu,ZOU Yi. On AES random transform masking scheme against DPA[J]. Journal of Cryptologic Reseatch, 2018,5(4):442-454.) doi:10.13868/j.cnki.jcr.000254.

[5] 史进,蔡竞,徐锋. 基于QR码与级联Fourier变换的图像光学加密算法[J]. 太赫兹科学与电子信息学报, 2020,18(3):462-469. (SHI Jin,CAI Jing,XU Feng. Multi-image optical encryption algorithm based on QR code and concatenated fractional Fourier transform[J]. Journal of Terahertz Science and Electronic Information Technology, 2020, 18(3): 462-469.) doi: 10.11805/TKYDA2019217.)

[6] 姚茂群,李聪辉. 基于预充电逻辑与掩码技术的功耗恒定性电路设计[J]. 杭州师范大学学报(自然科学版), 2022,21(2):184-189. (YAO Maoqun, LI Conghui. Design of circuit with constant power consumption based on precharge logic and masking technology[J]. Journal of Hangzhou Normal University(Natural Sciences Edition), 2022, 21(2): 184-189.) doi: 10.19926/j.cnki.issn.1674-232X.2022.02.012.

[7] 曹文龙. 双轨AES实现的安全性分析及防御对策的研究[D]. 合肥:中国科学技术大学, 2021. (CAO Wen. Research on security analysis and countermeasures of dual rail AES implementation[D]. Hefei,China:University of Science and Technology of China, 2021.)

[8] 蔡里昂. 抗DPA攻击功耗平坦化标准单元设计[D]. 天津:天津大学, 2019. (CAI Li'ang. Design of DPA-resistant power-flattening standard cells[D]. Tianjin,China:Tianjin University, 2019.)

作者简介：

李聪辉(1996-)，男，硕士，助教，主要研究方向为低功耗数字集成电路设计研究.email:liconghui96@qq.com.

姚茂群(1967-)，女，博士，教授，主要研究方向为低功耗数字集成电路设计研究.