DOI:10.11918/202103131

采用混合 MTJ/CMOS 和 SABL 结构的密码算法电路设计

王晨旭[1],闫 涛[1],宫月红[2],罗 敏[1],曾 琅[3],张德明[3],徐天亮[1]

(1. 哈尔滨工业大学(威海) 信息科学与工程学院,山东 威海 264209;2. 山东交通学院 航运学院,山东 威海 264200;
3. 北京航空航天大学 集成电路科学与工程学院,北京 100191)

摘 要: 为了在提高轻量级密码算法(Lightweight cipher algorithm,LWCA)电路安全性的同时降低功耗,提出了一种磁隧道结(Magnetic tunnel junction,MTJ)/CMOS 混合结构查找表(Look up table,LUT)电路,该结构通过与感测放大器逻辑(Sense amplifier based logic, SABL)元件配合可以实现完整的 PRESENT-80 加密算法电路。设计将 MTJ 器件引入防护电路设计中,进而提出了一种基于混合 MTJ/CMOS 结构的双轨查找表(Look-up table,LUT)电路结构。首先,基于 40 nm CMOS 工艺库和 MTJ 器件仿真模型,使用新提出的双轨查找表结构设计了加密算法电路工作过程中所需要的关键 S-box 电路并通过了仿真验证。然后,利用该电路和敏感放大器逻辑元件电路结构组合设计了 PRESENT-80 密码算法的完整电路。最后对所设计的电路模型进行了相关性功耗分析攻击(CPA)攻击,同时为了方便进行对比研究,还对使用传统 CMOS 单轨和 SABL 双轨结构实现的 PRESENT-80 加密算法电路模型进行了相同条件下的仿真和功耗分析研究。对比仿真结果表明,基于新结构实现的电路具有良好的抗功耗攻击性能,能够抵御 10 000 条功耗迹下的 CPA 攻击,同时新结构的电路在工作时的平均功耗要明显低于经典的 SABL 电路。

关键词: MTJ;SABL;PRESENT;低功耗;抗 CPA 攻击
中图分类号: TN43 **文献标志码:** A **文章编号:** 0367-6234(2022)06-0072-07

Circuit design of cryptographic algorithm using hybrid MTJ/CMOS and SABL structure

WANG Chenxu[1], YAN Tao[1], GONG Yuehong[2], LUO Min[1], ZENG Lang[3], ZHANG Deming[3], XU Tianliang[1]

(1. School of Information Science and Engineering, Harbin Institute of Technology (Weihai), Weihai 264209, Shandong, China;
2. School of Navigation and Shipping, Shandong Jiaotong University, Weihai 264200, Shandong, China;
3. School of Integrated Circuit Science and Engineering, Beihang University, Beijing 100191, China)

Abstract: To improve the circuit security of lightweight cipher algorithm (LWCA) and reduce power consumption, we proposed a look-up table (LUT) circuit with magnetic tunnel junction (MTJ)/CMOS hybrid structure, which can realize the complete PRESENT-80 encryption algorithm circuit by combining with sense amplifier based logic (SABL) cells. MTJ cells were introduced into the protection circuits for the design of the LUT circuit with hybrid MTJ/CMOS structure. Firstly, on the basis of 40 nm CMOS process and MTJ simulation model, the proposed LUT architecture was applied to design the S-box circuits which are essential in the operation process of cryptographic algorithm circuits, and results were verified through simulation. Secondly, a complete PRESENT-80 algorithm circuit was designed with the combination of the proposed circuit and SABL cells. Finally, all the circuits were tested by correlation power attack (CPA). Identical simulation and power consumption analysis were conducted on conventional CMOS single-rail and SABL dual-rail circuit structures. Results show that the proposed circuit possessed excellent power consumption attack resistance ability, which was capable of protecting against the CPA attack from 10 000 samples. Besides, the average power consumption of the proposed circuit was apparently reduced compared with that of the traditional SABL circuit.

Keywords: magnetic tunnel junction (MTJ); sense amplifier based logic (SABL); PRESENT; low power consumption; resistance to correlation power attack (CPA)

随着物联网(Internet of things, IoT)和传感器网络技术的快速发展,物联网嵌入式设备的集成度越来越高,对整体功耗的限制也越发严格。由于物联网通信中大量信息不断且频繁地传输,通信安全问题愈发受到人们的重视[1]。目前市场上的嵌入式

收稿日期: 2021-03-31
基金项目: 中国科学院 A 类战略先导专项项目(XDA19010302);国家自然科学基金(12075142,U2106202);山东省重大科技创新工程(2020CXGC010705,2021ZLGX05)
作者简介: 王晨旭(1977—),男,教授
通信作者: 宫月红,gongyuehonghit@126.com

设备主要使用轻量级密码算法(Lightweight cipher algorithm,LWCA)电路对传输信息进行加密。而随着半导体工艺的快速发展和功耗攻击技术的进步,传统的防护方法如加入掩码或提升算法复杂度[2-3]、使用防护基本单元[4-5]等方法均会带来面积和功耗上的巨大损耗,已经不能满足愈发严格的功耗和安全要求,市场上迫切需要一种兼具低功耗和高安全性的电路解决方案。针对当前现状和存在的问题,本文提出了一种 MTJ/CMOS 混合结构查找表电路,该结构通过与感测放大器逻辑(Sense amplifier based logic,SABL)元件配合可以实现完整的 PRESENT-80 加密算法电路。本文使用 Cadence 软件对设计电路进行仿真并提取电路的功耗信息进行了功耗分析攻击以研究其抗攻击性能。在研究过程中还使用相同的工艺库搭建了传统的 CMOS 单轨和 SABL 双轨结构的 PRESENT-80 电路来实现对比分析,通过一些评估参数的计算来对实验结果进行进一步的量化分析,探究该电路是否具备低功耗特性。

1　基本结构和加密算法

1.1　磁隧道结

MTJ 由于其良好的电学特性而在研究界引起了广泛的关注,它是由两个铁磁(FM,例如 CoFeB)层组成的纳米结构,铁磁层之间由氧化物阻挡层(例如,MgO)隔开,如图 1(a)所示[6]。铁磁层分为参考层和自由层,参考层的磁化方向是固定的,而自由层的磁化方向可以在平行(P)和反平行(AP)方向之间切换,其过程如图 1(b)所示。通过研究发现,当 MTJ 的铁磁层处于反平行状态时的电阻值(R_{AP})要明显大于处于平行状态的电阻值(R_P),衡量这种电阻特性的参数称为隧道磁阻(R_{TM})。R_{TM}的具体定义为$(R_{AP}-R_P)/R_P$[7]。

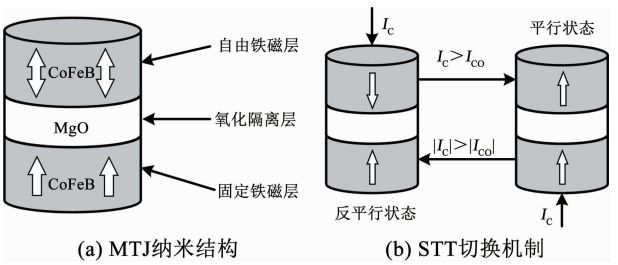

图 1　MTJ 结构与切换机制示意

Fig. 1　Schematic of MTJ structure and switching mechanism

本文中进行电路设计和仿真使用是基于开源网站 Spinmodel library 上提供的 STT PMA MTJ 仿真模型[8],其各项特性参数见表 1。

表 1　MTJ 模型的各项参数

Tab. 1　MTJ model parameters

玻尔兹曼常数 k_B/J	单位电荷 e/C	约化普朗克常数 $\hbar$/(J·S)	MgO 势垒高度 φ/eV	交换刚度 A_{ex}/(J·cm^{-1})	饱和磁化强度 M_s/(A·m^{-1})	各向异性场强 H_k/(A·cm^{-1})	面积电阻指数 RA/(kΩ·m^2)
1.38×10^{-23}	1.60×10^{-19}	1.055×10^{-34}	0.4	4×10^{-13}	8.0×10^{5}	3.6×10^{5}	5×10^{-12}

温度 T/K	自旋极化效率系数 g	MTJ 侧向直径 a/cm	MTJ 自由层厚度 d/cm	氧化层厚度 t_{ox}/cm	吉尔伯特阻尼因子 α	零偏置 TMR 比率/%
300	0.57	2.8×10^{-6}	0.85×10^{-7}	0.85×10^{-7}	0.036	100

1.2　SABL 逻辑

SABL 是一种经典的抗 DPA 逻辑结构,该结构由交叉耦合的反相器和差分下拉网络(Differential pull down network,DPDN)组成[9-10]。SABL 通用门电路和 AND-NAND 门电路如图 2 所示。整个电路由时钟信号 clk 驱动,当时钟电平为“0”时,两个输出信号端子都被预充为高电平;当时钟电平为“1”时,两个信号端子之一会根据输入的不同情况被置为低电平。恒定导通的晶体管 M_1通过用作亚阈值电流的路径来防止浮置节点,并保证所有内部节点都有放电通路[11-12]。

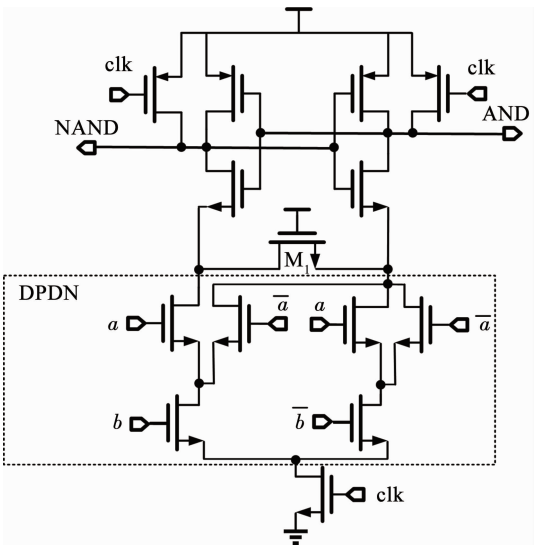

图 2　SABL 与非门示意图

Fig. 2　NAND gate diagram of SABL

1.3 PRESENT 算法

PRESENT 是一种轻量级分组加密算法，明文输入为 64 bit，密钥长度为 80 bit 或者 128 bit，密文输出为 64 bit。其加密过程包括 31 个常规循环和仅由密钥混合步骤组成的最终循环[13]，该算法的加密过程如图 3 所示。

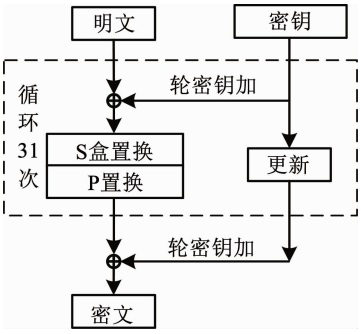

图 3 PRESENT 加密过程

Fig. 3 PRESENT encryption process

图中每轮循环过程需要经历 S 盒变换、P 置换、轮密钥加变换 3 种数据处理过程，且在最后一轮迭代完成后还需要再与轮密钥进行一次异或运算才能得到最终的密文。PRESENT 被广泛应用于低功耗电池供电的嵌入式设备中以进行加解密操作。

2 电路设计和仿真

2.1 多米诺机制

对 SABL 逻辑所述的交叉耦合反相器结构进行改进，得到的电路结构如图 4 所示，改进后电路的两输出端各加入了一个反向器。在时钟为“0”时输出信号将被置为“0”，这意味着在逻辑组件级联的计算阶段，下一级组件的 DPDN 中的 NMOS 晶体管不会被 GND 意外地导通。同时，逻辑功能和差分输出不会受到影响，这种信号传输机制称为多米诺机制[14]。

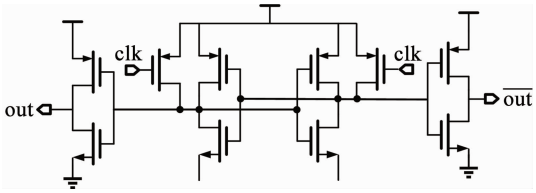

图 4 改进后的交叉耦合反相器结构

Fig. 4 Improved cross-coupled inverter structure

2.2 混合 MTJ/CMOS 结构 S-box 电路

S-box 电路是对被加密数据进行非线性变换的基本单元。每个 S-box 电路有 4 位输入和 4 位输出，其对应关系见表 2。

表 2 PRESENT-80 S-box 输入输出关系

Tab. 2 Input and output relationship of PRESENT-80 S-box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

本文提出了一种基于 MTJ/CMOS 的 LUT(look up table)电路结构，在该结构的设计中使用了多米诺机制，从而避免在与其他组件进行级联时信号逻辑发生错误。基于该结构设计的互补四输入的 LUT 电路如图 5 所示，该电路在工作开始之前，需要预先通过写入电路在 MTJ 中写入指定的数据。在电路工作时，会通过输入选择信号来定位到 LUT 中相应 MTJ 中存储的数据，并通过图 4 所示的多米诺机制的交叉耦合反相器将数据读取出来。与传统的 SRAM 等存储电路相比，将 MTJ 作为存储单元主要有两大优势。首先，使用传统方式实现 S-box 电路得到的电路会比较复杂，静态功耗大。而 MTJ 在工作时的静态电流几乎为零，因此使用 MTJ 进行设计能够大大降低了电路的功耗。其次，MTJ 是性能良好的非易失器件，在掉电的情况下其存储的信息也能长时间的保存，这样的特性恰恰与 S-box 电路相契合，因为非线性变换的输入与输出关系是固定的，数据写入后就不需要再被改写或者频繁刷新。如果使用 SRAM 一类的传统存储单元设计电路，则每次给电路通电时都必须刷新数据从而带来额外的功耗。

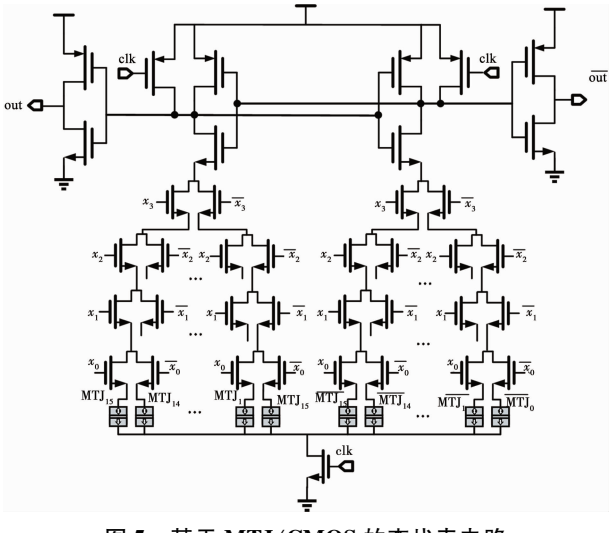

图 5 基于 MTJ/CMOS 的查找表电路

Fig. 5 Look-up table circuit based on MTJ/CMOS

Kumar 等[15]提出了一种使用基于混合 MTJ/CMOS 内存中逻辑 LUT 的电路实现 PRESENT-80 S-box 电路的方法，PRESENT-80 S-box 电路由 4 个的 LUT 电路组成，如图 6 所示，表 3 中显示了每个 LUT 中以 MTJ 编写的内容，该方法适用于低功耗硬件设

计[15-17]。然而，文献[15]中只实现了一轮加密过程，没有对密钥更新和电路级联问题给出明确的解决方案。针对这一问题，本文提出的电路结构可以与满足多米诺机制的标准 SABL 逻辑单元实现级联，很好的解决了这一问题，进而可以实现完整的加密电路设计。对于加密算法而言，满足此级联连接非常重要，因为由于整个算法中需要多次加密，数据会参照时钟进行频繁的迭代，因此 S-box 与其他逻辑单元之间的级联连接是必须的。

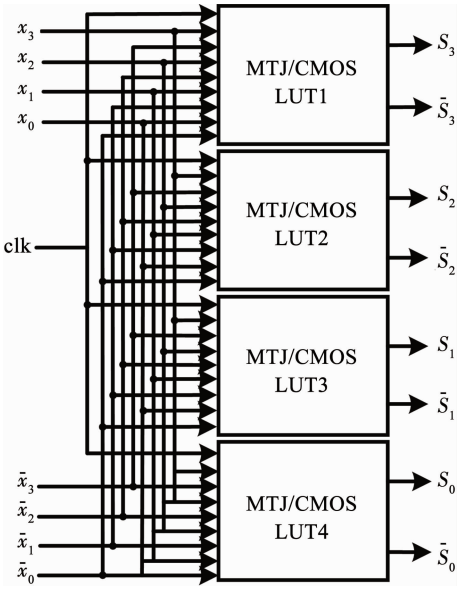

图 6　PRESENT-80 双轨 S-box 电路框图

Fig. 6　Block diagram of PRESENT-80 dual-rail S-box circuit

参考文献[15]中的结构用本文提出的查找表电路设计了 S-box 电路。基于 SMIC 40 nm CMOS 工艺和 MTJ 仿真模型在 Cadence Spectre 模拟器中对 S-box 电路进行功能仿真。在仿真过程中，从选择信号端输入由 0x0 到 0xF 的多米诺机制激励，最终获得的仿真结果如图 7 所示。分析图像可以看出当时钟为“0”时，所有信号均被驱动为“0”。相反，当时钟为“1”时，信号代表的逻辑值对应关系与表 2 完全一致，证明所设计的电路功能是完全正确的。

2.3　PRESENT-80 加密电路的实现

图 8 显示了 PRESENT-80 的一轮加密过程，可以看出除了密钥输入部分和 S-box（S_{15} ~ S_0）之外，算法的实现还需要大量异或门。标准 PRESENT-80 算法中的密钥每轮都会迭代更新，如果使用 MTJ/CMOS 结构电路实现这些异或门，则会带来额外的能量损失同时提高被功耗攻击的风险。因此最终选择使用满足多米诺机制 SABL 异或门来完成该部分的逻辑实现。

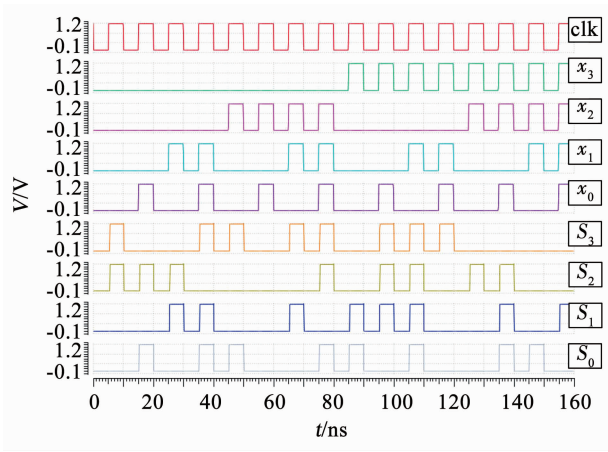

图 7　MTJ/CMOS S-box 电路仿真结果

Fig. 7　MTJ/CMOS S-box circuit simulation results

表 3　查找表电路中各 MTJ 存储数据

Tab. 3　MTJ stored data in look-up table circuit

MTJ	LUT1	LUT2	LUT3	LUT4
MTJ_0	1	1	0	0
MTJ_1	0	1	0	1
MTJ_2	0	1	1	0
MTJ_3	1	0	1	1
MTJ_4	1	0	0	1
MTJ_5	0	0	0	0
MTJ_6	1	0	1	0
MTJ_7	1	1	0	1
MTJ_8	0	0	1	1
MTJ_9	1	1	1	0
MTJ_{10}	1	1	1	1
MTJ_{11}	1	0	0	0
MTJ_{12}	0	1	0	0
MTJ_{13}	0	1	1	1
MTJ_{14}	0	0	0	1
MTJ_{15}	0	0	1	0

同样用 Cadence Spectre 模拟器来模拟 PRESENT-80 电路的完整工作过程。在仿真过程中为了节省仿真资源，算法中除去关键的轮加密部分电路外的执行其他数据处理任务的电路使用硬件描述语言建立功能模型的方式代替。在仿真中，原始的明文设置为 0x0044003300220011，原始密钥设置为 x0123456789ABCDEF0123。图 9 显示了 32 轮加密过程中部分密文输出信号的仿真波形。经过检查该结果与相同输入情况下标准算法的处理结果完全一致，由此可以证明本文设计的电路可以正确实现 PRESENT-80 加密算法电路的功能。

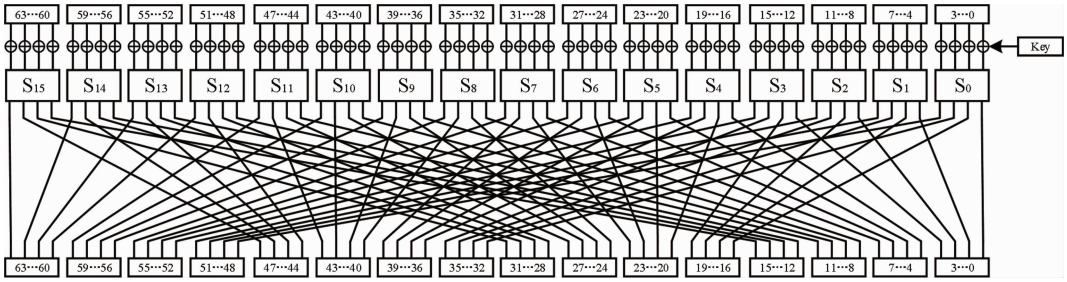

图 8 一轮 PRESENT-80 加密过程框图

Fig. 8 Block diagram of a round of PRESENT-80 encryption process

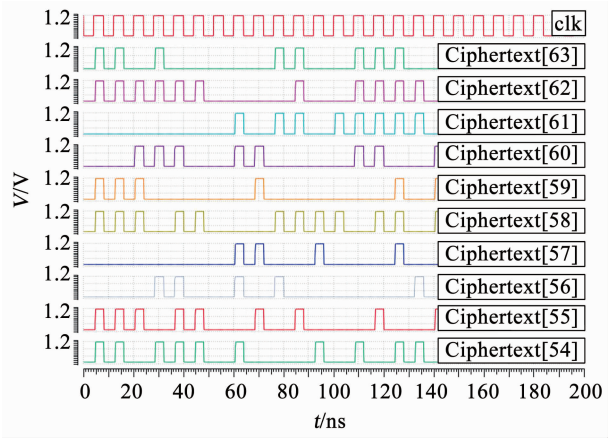

图 9 32 轮加密过程中部分密文信号的波形

Fig. 9 Waveform of part of ciphertext signal during 32 rounds of encryption

3 电路性能评估和分析

要验证本文所设计的电路结构是否具备良好的抗攻击特性,需要对电路进行功耗攻击分析测试。学者 Kocher[18] 最早提出了差分功耗攻击(Differential power analysis, DPA)的概念。DPA 攻击利用了电路中由晶体管功耗变化引起的功耗波动来分析加密电路信息。通过跟踪这些波动并分析电路特定部分的功耗就可以获得加密信息(例如密钥),同时不会影响设备的任何物理特性[19]。本文选取了一种改进型的差分功耗攻击模型,即相关性功耗分析攻击(Correlation power attack, CPA)模型[20],该模型在使用中需要选择合适的攻击点测量得到功耗信息矩阵,与假设功耗矩阵进行对比得到它们之间的相关系数,相关系数最高的便是密钥值。基于 10 000 条功耗迹对传统 CMOS 单轨 PRESENT-80 电路进行 CPA 攻击,设定的攻击目标为首轮加密的 64 bit 密钥,其真实值为 0x0123456789ABCDEF。攻击过程分 16 组,每组攻击 4 bit,攻击的结果如图 10所示,其中左侧为攻击每组密钥的相关系数曲线,右侧为攻击第 47 ~44 位密钥过程中相关系数与功耗迹条数的关系曲线,其中深色曲线为真实密钥的相关系数曲线。结果显示,真实密钥被成功破解,且确保攻击成功所需要的功耗迹条数在 1 000 条左右。

使用相同的攻击模型对本文中所设计的密码算法电路进行 CPA 攻击,其攻击结果如图 11 所示,攻击得到的首轮密钥值为 0xD1009B00D6009100,攻击未成功,同时可以看出真实密钥的相关性一直被很好的隐藏与各猜测密钥之中且随着功耗迹数目的增加相关性变化趋于稳定。对比上述结果,可以证明本文中设计的电路结构具有良好的抗攻击性能。

为了便于对逻辑单元的抗功耗攻击性能进行量化分析,需要统一的衡量指标。目前普遍使用的评估标准主要有如下几种[5]:

1)归一化功耗差(Normalized energy deviation, NED)。

$$\mathrm{NED} = \frac{E_{\max} - E_{\min}}{E_{\max}} \tag{1}$$

式中,$E_{\max}$、$E_{\min}$分别为电路在电路单个周期内的功耗的最高值和最低值,定义如下:

$$E = V_{\mathrm{DD}} \cdot \overline{I} \cdot T_{\mathrm{CLK}} = V_{\mathrm{DD}} \cdot \int_0^T I_{\mathrm{DD}}(t)\,\mathrm{d}t$$

2)归一化标准差(Normalized standard deviation, NSD)。

$$\mathrm{NSD} = \frac{\sigma_{\mathrm{E}}}{\overline{E}} \tag{2}$$

3)归一化电流差(Normalized current deviation, NCD)。

$$\mathrm{NCD} = \frac{C_{\max} - C_{\min}}{C_{\max}} \tag{3}$$

式中,$C_{\max}$、$C_{\min}$分别为每个参考周期的峰值电流的最高值和最低值。

根据功耗攻击的原理可以发现,目标电路的 NED,NSD 和 NCD 数值越低,抗攻击的特性就越好。对 PRESENT-80 加密电路的工作过程进行仿真可以提取加密算法电路的工作电流,并以此计算出相应的 NED,NSD 和 NCD。为了便于进行比较和分析,本文在相同的仿真环境下建立了另外两套基于 40 nm CMOS 工艺的 PRESENT 加密电路模型,分别使用了传统的单轨 CMOS 逻辑单元和 SABL 逻辑单元在相同的实验条件下设计了加密电路模型并完成了仿真。所有电路仿真后得到的电流数据如图 12 所示,基于此计算出的抗攻击评估指标和 $\overline{E}$ 见表 4。

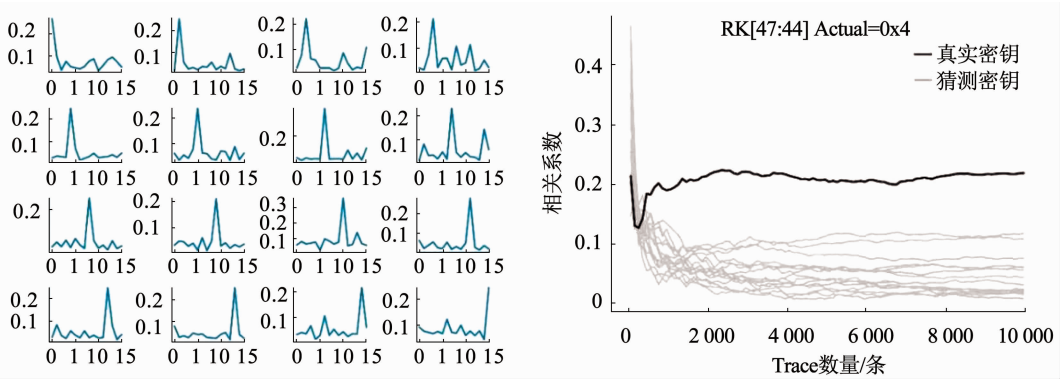

图 10　PRESENT-80 单轨电路 CPA 攻击结果

Fig. 10　CPA attack results of PRESENT-80 single-rail circuit

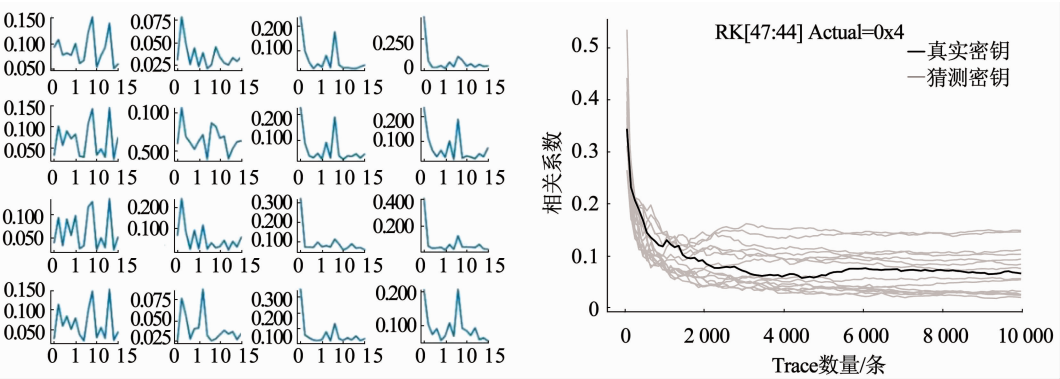

图 11　MTJ/CMOS PRESENT-80 电路 CPA 攻击结果

Fig. 11　CPA attack results of MTJ/CMOS PRESENT-80 circuit

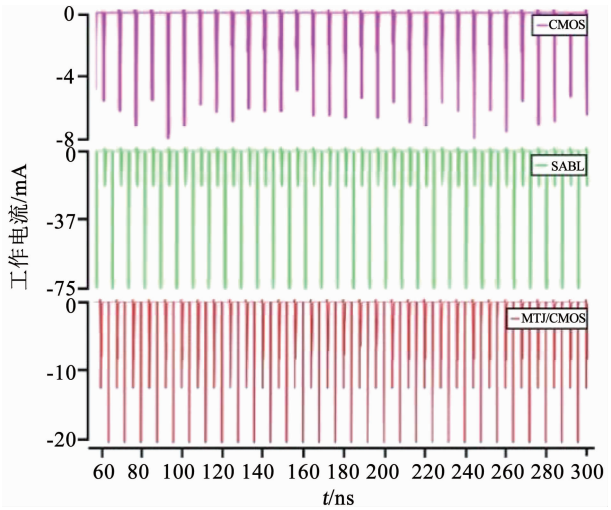

图 12　不同电路的工作电流仿真结果

Fig. 12　Simulation results of power supply current of different circuits

表 4　PRESENT-80 的 CMOS、SABL 和 MTJ/CMOS 电路的评估指标

Tab. 4　Evaluation indicators of CMOS, SABL, and MTJ/CMOS circuits for PRESENT-80

指标	NED/%	NSD/%	NCD%	$\overline{E}$/pJ
CMOS	33.060	1.907	44.910	2.42
SABL	0.110	0.007	0.050	12.59
MTJ/CMOS	0.390	0.004	0.030	5.64

从 3 种电路仿真计算得出的 NED、NSD 和 NCD 比较中可以看出，使用 MTJ/CMOS 结构 S-box 电路设计的电路的抗攻击特性与 SABL 标准单元加密电路相近，且明显优于传统的 CMOS 电路。同时，含 MTJ/CMOS 结构的加密电路的平均功耗 $\overline{E}$ 高于传统的单轨 CMOS 电路，但是其功耗要显著低于 SABL 结构电路。综上所述，本文提出的基于 MTJ/CMOS LUT 结构和改进后 SABL 单元设计的 PRESENT 加密算法电路可以在不增加过多功耗的前提下显著提高电路的抗攻击能力，具有一定的性能优势。

4　结　论

1）本文提出的混合 MTJ/CMOS 结构的 LUT 电路能够正确实现密码算法中 S-box 的功能，并且可以与符合多米诺级联机制的 SABL 电路进行级联电路设计。

2）混合 MTJ/CMOS 结构 LUT 电路具有良好的电路级防护性能，使用其设计的密码算法电路能够抵御 10 000 条功耗迹的 CPA 攻击。

3）在同等工艺条件下，使用混合 MTJ/CMOS 结构设计的密码电路相较于传统的 SABL 结构电路功耗会有显著的降低。

参考文献

[1] SHEBLI H M Z A, BEHESHTI B D. Light weight cryptography for resource constrained IoT devices[J]. Advances in Intelligent Systems and Computing, 2019(880): 196. DOI: 10.1007/978-3-030-02686-8_16

[2] NIKOVA S, RIJMEN V, SCHLÄFFER M. Secure hardware implementation of nonlinear functions in the presence of glitches[J]. Journal of Cryptology, 2011, 24(2): 292. DOI: 10.1007/s00145-010-9085-7

[3] BILGIN B, NIKOVA S, NIKOV V, et al. Threshold implementations of small S-boxes[J]. Cryptography and Communications, 2015, 7(1): 3. DOI: 10.1007/s12095-014-0104-7

[4] TIRI K, VERBAUWHEDE I. A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation [C]// Proceedings Design, Automation and Test in Europe Conference and Exhibition. Paris, France: IEEE, 2004: 246. DOI: 10.1109/DATE.2004.1268856

[5] 吴静. 抗 DPA 攻击的标准单元库及密码算法的研究与实现[D]. 长沙: 国防科学技术大学, 2010
WU Jing. The research and implementation of DPA-resistant standard cells and encryption arithmetic[D]. Changsha: National University of Defense Technology, 2010

[6] YUASA S, NAGAHAMA T, FUKUSHIMA A, et al. Giant room-temperature magnetoresistance in single-crystal Fe/MgO/Fe magnetic tunnel junctions[J]. Nature Materials, 2004, 3 (12): 868. DOI: 10.1038/nmat1257

[7] WANG Kang, ZHANG Yue, WANG Zhaohao, et al. Spintronics: Emerging Ultra-Low-Power circuits and systems beyond MOS technology [J]. ACM Journal on Emerging Technologies in Computing Systems, 2015, 12(2): 1. DOI:10.1145/2663351

[8] MOODERA J S, KINDER L R, WONG T M, et al. Large magnetoresistance at room temperature in ferromagnetic thin film tunnel junctions[J]. Physical Review Letters, 1995, 74(16): 3273. DOI: 10.1103/PhysRevLett.74.3273

[9] WANG You, CAI Hao, NAVINER L A D B, et al. Compact model of dielectric breakdown in spin transfer torque magnetic tunnel junction [J]. IEEE Transactions on Electron Devices, 2016, 63(4): 1762. DOI: 10.1109/TED.2016.2533438

[10] TIRI K, VERBAUWHEDE I. Design method for constant power consumption of differential logic circuits[C]//Design, Automation & Test in Europe. Munich, Germany: IEEE, 2005: 628. DOI: 10.1109/DATE.2005.113

[11] 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]// Proceedings of the 28th European Solid-State Circuits Conference. Florence, Italy: IEEE, 2002: 403

[12] KIM J C, JANG Y C, PARK H J. CMOS sense amplifier-based flip-flop with two N-(CMOS)-M-2 output latches[J]. Electronics Letters, 2000, 36(6): 498. DOI: 10.1049/el:20000409

[13] TIRI K, VERBAUWHEDE I. Charge recycling sense amplifier based logic: Securing low power security IC's against DPA[C]// Proceedings of the 30th European Solid-State Circuits Conference. Leuven, Belgium: IEEE, 2004: 179. DOI: 10.1109/ESSCIR.2004.1356647

[14] BOGDANOV A, KNUDSEN L R, LEANDER G, et al. PRESENT: An Ultra-Lightweight block cipher[C]//Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer, 2007: 450. DOI: 10.1007/978-3-540-74735-2_31

[15] KUMAR S D, THAPLIYAL H. Exploration of non-volatile MTJ/CMOS circuits for DPA-resistant embedded hardware[J]. IEEE Transactions on Magnetics, 2019, 55(12): 1. DOI: 10.1109/TMAG.2019.2943053

[16] MANGARD S, OSWALD E, POPP T. Power analysis attacks-revealing the secrets of smart cards[M]. Berlin, Heidelberg: Springer Publishing Company, 2010

[17] ZHAO Weisheng, Moreau M, DENG E, et al. Synchronous non-volatile logic gate design based on resistive switching memories[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2014, 61(2): 443. DOI: 10.1109/TCSI.2013.2278332

[18] KOCHER P, JAFFE J, JUN B. Differential power analysis[C]// Proceedings of the Annual International Cryptology Conference. Berlin Heidelberg: Springer, 1999: 388. DOI: 10.1007/3-540-48405-1_25

[19] WINOGRAD T, SALMANI H, MAHMOODI H, et al. Hybrid STT-CMOS designs for reverse-engineering prevention[C]//Proceedings of the 53nd ACM/EDAC/IEEE Design Automation Conference (DAC). Austin, TX: IEEE, 2016: 5. DOI: 10.1145/2897937.2898099

[20] DUAN Xiaoyi, CU Qi, WANG Sixiang, et al. Differential power analysis attack and efficient countermeasures on PRESENT[C]// Proceedings of 2016 8th IEEE International Conference on Communication Software and Networks. Beijing: IEEE, 2016: 8. DOI: 10.1109/ICCSN.2016.7586627

[21] 王晨旭, 赵占锋, 喻明艳, 等. Piccolo 相关性功耗分析攻击技术研究[J]. 哈尔滨工业大学学报, 2013, 45(9): 17
WANG Chenxu, ZHAO Zhanfeng, YU Mingyan, et al. Research on correlation power analysis attack against Piccolo[J]. Journal of Harbin Institute of Technology, 2013, 45(9): 17. DOI: 10.11918/j.issn.0367-6234.2013.09.004

(编辑 张 红)