

引用格式:李凯利,张卫航,郭桂良. 基于 Bus-Invert 编码的低功耗 AES 加密电路设计[J]. 微电子学与计算机, 2019, 36(7): 27-31. [LI K L, ZHANG W H, GUO G L. Design of low power AES encryption circuit based on bus-invert coding[J]. Microelectronics & Computer, 2019, 36(7): 27-31.]

基于 Bus-Invert 编码的低功耗 AES 加密电路设计

李凯利¹, 张卫航², 郭桂良¹

(1 中国科学院大学 微电子学院, 北京 100049; 2 中芯国际集成电路制造有限公司, 上海 201210)

摘 要: 随着无线设备的广泛应用, 半导体应用市场对低功耗加密电路提出了更高的要求. 降低功耗可以延长无线设备的工作时间以及待机时间, 而加密电路能够保障数据传输的安全性. 在低功耗设计方法中, 通过对信号编码来降低信号翻转率具有重要的研究意义. BI(Bus-Invert)编码技术可以降低随机信号的翻转率, 在 AES 加密电路中引入 BI 编码技术, 对电路输入数据 BI 编码, 可得到一种改进型的低功耗 AES 加密电路. 经验证, 与原电路相比, 改进型电路的 ShiftRow、MixColumn、SubByte、KeyExpansion 各子模块每周期内的平均翻转率分别降低了 68%、42%、50%、46%, 动态功耗降低了 36.4%.

关键词: Bus-Invert 编码; 低翻转率; 低功耗; AES 加密电路

中图分类号: TN492

文献标识码: A

文章编号: 1000-7180(2019)07-0027-05

Design of low power AES encryption circuit based on Bus-Invert coding

LI Kai-li¹, ZHANG Wei-hang², GUO Gui-liang¹

(1 School of Microelectronics, University of Chinese Academy of Science (UCAS), Beijing 100049, China;

2 Semiconductor Manufacturing International Corporation (SMIC), Shanghai 201210, China)

Abstract: With the widespread use of wireless devices, the semiconductor application market has placed higher demands on low-power encryption circuits. Reducing power consumption can extend the operating time and standby time of wireless devices, while encryption circuits ensure data transmission security. In the low-power design method, it is of great research significance to reduce the signal toggle rate by coding the signal. BI (Bus-Invert) [1] coding technology can reduce the toggle rate of random signals. By introducing BI coding technology in AES encryption circuit and encoding input data, an improved low-power AES encryption circuit can be obtained. It is verified that compared with the original circuit, the average toggle rate of the ShiftRow, MixColumn, SubByte, and KeyExpansion sub-modules of the improved circuit is reduced by 68%, 42%, 50%, and 46%, respectively, and the dynamic power consumption is reduced 36.4%.

Key words: Bus-Invert coding; reduce the toggle rate; low power consumption; AES encryption circuit

1 引言

随着集成电路制造工艺的发展, 集成电路的集成度和性能飞速提高, 芯片功耗在系统中的影响越来越大. 降低功耗不但可以降低芯片的散热和封装

成本, 而且可以减少系统故障, 提高系统可靠性. 所以低功耗电路设计有着重要的研究意义^[1].

CMOS 电路中的功耗主要有以下四大来源: 功能跳变、短路电流、竞争冒险、漏电流. 前三种统称为动态功耗 (Dynamic Power), 是由电路正常工作时

信号翻转引起的. 漏电流产生的功耗称为静态功耗 (Static Power), 电路中的功耗由动态功耗和静态功耗组成. 动态功耗是由电路中信号翻转引起的, 降低信号的翻转率是降低动态功耗的有效方法, SoC 数据总线中常用的 BI 编码技术可以降低随机数据的翻转率, 将 BI 编码技术应用到逻辑运算之前, 先对输入数据 BI 编码, 然后再逻辑运算. AES 加密电路的运算逻辑比较复杂, 电路中信号的翻转率比较高, 可以将这一方法用在 AES 电路中.

AES 加密算法是一种迭代分组加密算法, 具有安全性能高、加密效率高、易于实现、灵活性强等优点, 广泛应用于计算机通信等各个领域. 2001 年 11 月, 美国国家标准技术研究所 (National Institute of Standard and Technologies, NIST) 选定 Rijndael 算法作为新的高级加密标准 (Advanced Encryption Standard, AES)^[2], 用来代替 DES 加密算法.

在低功耗 AES 加密电路设计中, Guido Bertoni 等人提出了一种解码 (Decode)-置换 (Permutation)-编码 (Encode) 的 SBox 硬件架构^[3], 该架构对 SBox 电路的输入数据 One-Hot 编码, 达到降低输入数据翻转率的目的. 但 One-Hot 编码后, 会增加输入数据的位宽, 导致置换电路的面积增加. Jinyi Zhang 等人采用 Sequence-Switch Coding (SSC) 技术对 SBox 输入数据进行编码^[4], 这种编码方式将 SBox 电路的输入数据重排次序, 排序后数据的翻转率降低. 但编码电路占用的时钟周期较多, 使加密速度变慢. 上面提到的两种方法均是对 SBox 电路输入数据编码, 本文设计了一种新的低功耗 AES 加密电路, 在 AES 加密电路之前增加 BI 编码电路, 对输入数据 BI 编码, 该方法在保证电路面积和速度性能变化较小的情况下, 可以更加有效地降低输入信号的翻转率.

2 降低翻转率编码技术和 AES 算法电路实现

2.1 降低翻转率编码技术

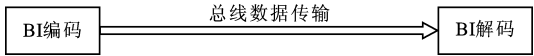
CMOS 电路动态功耗表达式如公式 (1) 所示.

$$P_d = \frac{1}{2} v_{dd}^2 f \sum_{i=1}^n a_i c_i \tag{1}$$

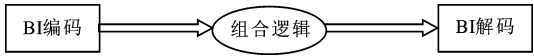
式中, v_{dd} 是电源电压; f 是系统频率; c_i 是节点 i 处的负载电容; a_i 是单个周期内信号的翻转率; n 是节点个数. 由公式 (1) 可知: 电路动态功耗和 v_{dd} 、 f 、 a_i 、 c_i 有关, 减小翻转率 a_i 可以降低动态功耗. 在电路的 RTL 级可以通过插入门控时钟的方法来减少信号的翻转. 在算法级和体系结构级可以通过编码

技术来减少信号的翻转, 比如对 SoC 数据总线上的数据 BI 编码. 地址总线传输的数据有很强的连续性, 可以采用 Gray 码^[5] 技术进行编码, 相邻的 Gray 码只有一位变化, 所以翻转率比较低. 在状态机中可以用 One-Hot 编码^[6] 技术对状态编码, One-Hot 编码后的数据只有 1 位为高电平, 其余位均为低电平, 每次状态转移有 2 位信号跳变.

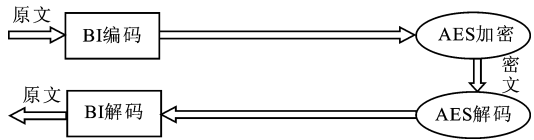
对于 BI 编码技术, 如图 1(a) 所示, 数据经 BI 编码, 然后通过数据总线传输, 在接收端对数据 BI 译码, 得到原始数据. 如果将这种编码方式用在图 1 (b) 所示的电路中, 先对数据进行 BI 编码, 编码后的数据进行逻辑运算, 最后将运算结果译码, 并不能得到期望的输出结果 (数据未经 BI 编码直接逻辑运算得到的结果). 但是对于加密电路而言, 如图 1(c) 所示, 原文经 BI 编码后, 通过 AES 加密电路得到密文, 此密文与只进行 AES 加密 (不加 BI 编码模块) 得到的结果不同, 但密文经过 AES 解密电路和 BI 译码电路可以得到原文. 针对这一特点, 可以将 BI 编码技术用在 AES 加密电路中.



(a)BI 编码电路应用在总线电路



(b)BI 编码电路应用在逻辑运算电路



(c)BI 编码电路应用在 AES 加密电路

图 1 BI 编码电路应用

2.2 AES 算法电路实现

AES 电路多采用并行结构和流水线结构, Hyun Suk Choi 等人提出了一种低功耗的 AES 并行电路结构^[7], 该结构有两个加密块同时进行加密操作, 使得数据吞吐量增加一倍, 相对于非并行结构的电路, 在数据处理速度相同的情况下, 并行结构电路的时钟频率可以降为原来的一半, 供电电压也可以降低, 从而降低电路功耗. 而 Salma Hesham 等人提出了一种流水线结构的电路^[8], 通过在加密主电路和密钥扩展电路中插入三级流水线寄存器, 同样可以提高数据处理速度, 并且在满足数据处理速度的基础上降低频率和供电电压. 此外, 许多研究人员

提出了新的硬件结构. 从原来的 128 位结构的 AES 电路,发展出了 32 位^[9]、16 位、8 位^[10]结构的电路,这些结构下的电路面积变小,功耗变低,但数据处理速度变慢. 在 AES 电路中,SubByte 运算是唯一的非线性运算,其电路设计比较复杂,并且占用较多的硬件资源,所以 SBox 电路是 AES 电路低功耗设计的热点^[3-4].

一种基本的 AES 加密电路硬件架构如图 2 所示:第 0 轮时,原文或密文经数据选择器 MUX1 输入到寄存器 DataReg 中,并且先与 UserKey 异或. 第 1-10 轮操作时,每轮可分为 3 步完成:

(1) 将 DataReg 中数据送入到 SubByte/InvSubByte 模块进行字节置换或者字节置换逆运算操作;

(2) 通过选择器 MUX2 模块将进行加密或者解密的数据送入到 ShiftRow/InvShiftRow 模块来完成行移位或者行移位逆运算操作;

(3) 将得到的数据通过选择器 MUX3 输出到 MixColumn/InvMixColumn 模块,若此时进行的是加密操作,并且不是最后一轮操作,那么 MUX3 中输出的数据首先与轮密钥 RoundKey 异或,然后进入 MixColumn 模块完成列混合运算,最后将结果通过选择器 MUX4 和 MUX5 输出;若此时进行的是解密操作,并且不是最后一轮操作,那么 MUX3 中的数据首先输入到 InvMixColumn 模块完成列混合逆运算,然后将得到的结果与 RoundKey 异或,异或后的结果通过选择器 MUX4 和 MUX5 输出;若此时进行的是最后一轮的加密或者解密操作,那么 MUX3 中输出的数据先与 RoundKey 异或,然后经选择器 MUX5 输出.

AES 加密时 1-9 轮进行周期性的运算,第十轮运算仅仅少了 MixColumn 操作. 为了减小芯片的面积和功耗,采用数据依次经过 SubByte、ShiftRow、MixColumn 等模块的逻辑复用结构,数据输出作为下一轮的数据输入进行循环迭代运算.

3 基于 BI 编码的改进型 AES 加密电路

对于无线传感器网络和物联网的一些终端设备,采集到的数据可能会只进行加密处理,数据的解密在一些专门的数据处理中心(如服务器)上完成,所以在这些场景中可以只对加密电路做低功耗设计. 本文设计了一种低功耗 AES 加密电路,有效降低了数据加密时的功耗,如图 3 所示,在 AES 每一轮数据运算时,先对输入的数据 BI 编码,其编码方

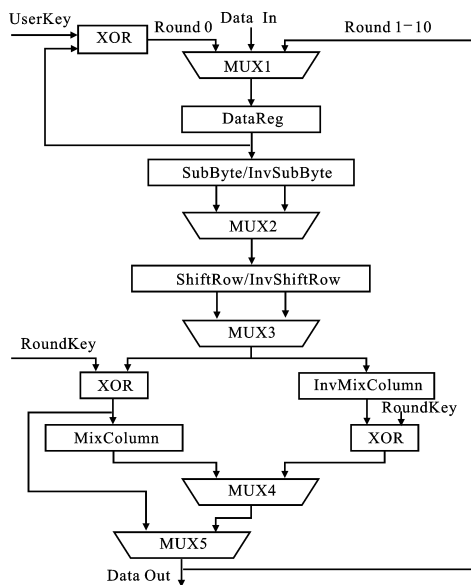


图 2 一种基本 AES 硬件设计架构

式是:计算输入数据当前码字和前一个码字之间的汉明距离,然后将求得的汉明距离与设定的阈值(输入数据位宽的一半)相比较,若两个码字之间的汉明距离大于所设定的阈值,则将输入的数据按位取反,这样两个码字之间的汉明距离就会小于所设定的阈值,从而降低了输入信号的翻转. 输出数据的同时输出一位标志位 C,若输入信号进行了取反操作,则标志位置为 1,否则标志位置为 0. 在解码时由标志位来决定是否对解码输入信号进行取反操作.

改进型 AES 加密电路(如图 3 所示)是在图 2 电路的基础上增加了 BIE(Bus_Invert_Encode)模块和 BID(Bus_Invert_Decode)模块. 如果是加密操作,选择器 MUX2 会将经 BIE 模块运算过的数据寄存到 DataReg 中,如果是解密操作,选择器 MUX2 选择 MUX1 中的数据寄存到 DataReg 中. 同时,在每轮运算的最后,增加一个 BID 模块和一个 MUX7 模块,当进行加密操作时,选择器 MUX7 选择 MUX6 中的数据作为输出,当进行解密操作时,选择器 MUX7 选择经 BID 模块运算过的数据作为输出. 其中 BIE 和 BID 模块的电路结构如图 4 和图 5 所示:BIE 模块首先将 Data_In 输入到寄存器 Data_Reg 之中,然后将 Data_Reg 中的数据和下一个时钟周期要输入的数据按位异或,对于这两组数据,如果数据对应的某一位相同,则异或之后为 0,若数据对应的某一位不同,则异或之后为 1,下一步将异或结果求和,求和结果正是两组数据间的汉明距离. 第四步进行逻辑判断,若求和结果大于所设定的阈值,则下一个周期要输入到 BIE 模块的数据按位取反,标

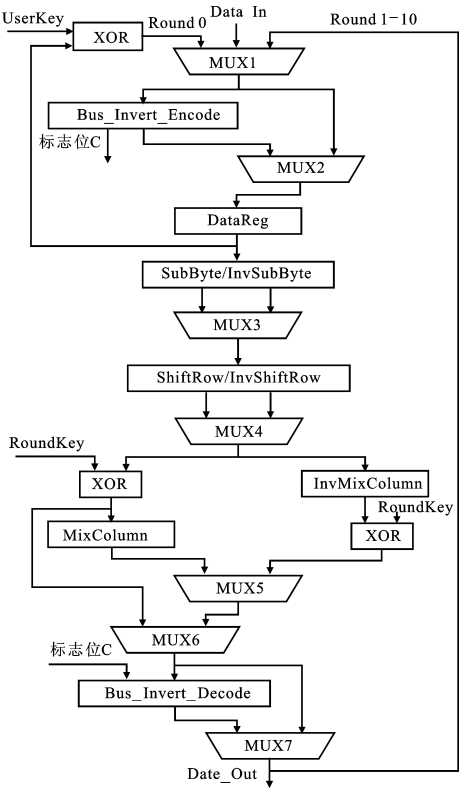


图 3 采用 BI 编码的改进型 AES 硬件设计架构

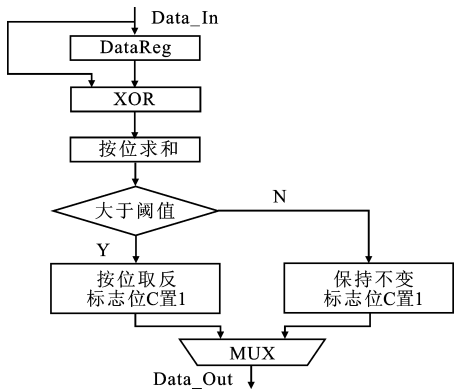


图 4 Bus_Invert_Encode 电路结构图

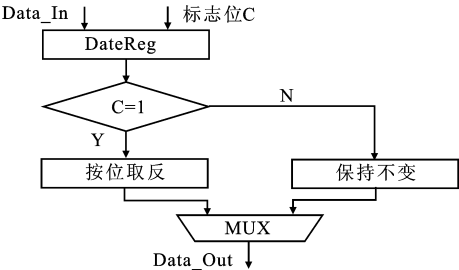


图 5 Bus_Invert_Decode 电路结构图

志位 C 置 1,若求和结果小于或等于所设定的阈值,则下一个周期要输入到 BIE 模块的数据不做任何处理,标志位 C 置 0. 对于 BID 模块,首先将输入

Data_In 和标志位 C 输入到寄存器 Data_Reg 中,第二步判断 C 的值是否为 1,若 C 的值为 1,则将 Data_Reg 中的数据按位取反输出,若 C 的值为 0,则将 Data_Reg 中的数据直接输出.

4 仿真结果及分析

对于改进型电路和未改进的 AES 电路,先用 Verilog 编写 RTL 代码,然后用 Synopsys 公司的 Design Compiler 工具综合成门级电路,在 Design Compiler Topographical 式下提取时序、寄生参数等信息,用 Synopsys 公司 vcs 工具对网表仿真,提取出翻转率信息. 然后用 PrimeTime PX 工具在 Time_Based 模式下生成功耗信息.

未改进电路和改进型电路各子模块每周期内的平均翻转率如表 1 所示. 每周期内的平均翻转率由公式(2)表示,平均翻转率等于每周期内跳变信号的个数与信号总数的比值,信号的平均翻转率可以表示出信号的跳变程度.

AverageToggle Rate=
$$\frac{\text{Number of Toggles on All Signals Per Interval}}{\text{Number of Signals}} \quad (2)$$

表 1 各子模块每周期内平均翻转率

电路类型	ShiftRow	MixColumn	SubByte	Key Expansion
未改进电路	0.36	0.45	0.32	0.39
改进型电路	0.13	0.26	0.16	0.21

图 6 是表 1 中数据对应的柱状图,从柱状图中可以更加直观地看到,相对于未改进的电路,改进型电路中 ShiftRow、MixColumn、SubByte、KeyExpansion 等模块的平均翻转率明显降低了. 改进型电路中的 ShiftRow、MixColumn、SubByte、KeyExpansion 各子模块每周期内的平均翻转率分别降低了 68%、42%、50%、46%.

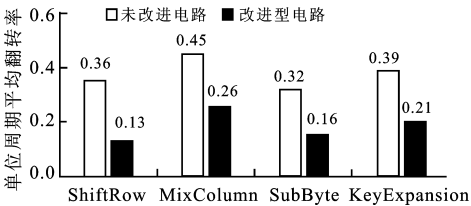


图 6 电路主要模块翻转率

动态功耗与翻转率有关,降低信号翻转率,电路功耗也应该随之降低. 表 2 中展示了未改进电路和改进型电路 Internal Power、Switching Power、Leakage Power、Total Power 的值. Internal Power 为短路功耗,即 PMOS 和 NMOS 同时导通时的功

耗. Switching Power 为开关功耗. Leakage Power 为漏电功耗. 动态功耗(Dynamic Power)等于短路功耗(Internal Power)与开关功耗(Switching Power)之和. 图 7 是表 2 对应的功耗柱状图,从中可以直观地看到电路中的功耗主要是短路功耗和开关功耗. 改进型电路中短路功耗和开关功耗都有所下降,改进后电路的短路功耗和开关功耗相较于未改进电路分别降低了 31. 3%, 43. 6%, 动态功耗降低了 36. 4%, 而漏电功耗所占比重较小,只是略微变高. 所以本文提到的改进型 AES 加密电路达到了降低动态功耗的目的.

表 2 电路动态功耗、静态功耗及总功耗表

电路类型	Internal Power/mW	Switch Power/mW	leakage Power/mW	Total Power/mW
未改进电路	6. 445 78	6. 183 48	0. 080 509	12. 7
改进型电路	4. 426 68	3. 490 29	0. 091 968	8. 01

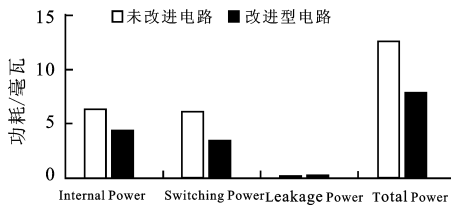


图 7 电路动态功耗、静态功耗及总功耗柱状图

5 结束语

利用 BI 编码技术可以降低信号翻转率,本文提出了一种改进型的低功耗 AES 加密电路,在 AES 电路中加入 BI 编码电路,每轮加密操作之前先对输入数据编码,然后再对编码后数据加密. 编码后数据翻转率降低,使得加密电路的动态功耗降低. 从仿真结果可知,AES 加密电路的动态功耗占了很大的比重. 与原电路相比,改进型电路中的 ShiftRow、Mix-Column、SubByte、KeyExpansion 各子模块每周期内的平均翻转率分别降低了 68%、42%、50%、46%,动态功耗降低了 36. 4%电路以牺牲较小的面积和速度性能为代价,换取了动态功耗的显著降低.

参考文献:

[1] FLETCHER R J. Integrated circuit having outputs configured forreducedstate changes; U. S. Patent 4667337[P]. 1987-5-19.

[2] NIST. FIPS PUBS 197. Advanced Encryption Stand-

ard (AES)[S]. America: National Institute of Standards and Technology, 2001.

[3] BERTONI G, MACCHETTI M, NEGRI L, et al. Power-efficient ASIC synthesis of cryptographic sboxes[C]// Acm Great Lakes Symposium on VLSI. Boston: ACM, 2004:277-281.

[4] ZHANG J Y, ZUO Q H, ZHANG T B. Reducing the power consumption of the AES S-Box by SSC[C]// International Conference on Wireless Communications, Networking and Mobile Computing. Shanghai: IEEE, 2007:2226-2229.

[5] MEHTA H, OWENS R M, IRWIN M J. Some issues in gray code addressing[C]// Proceedings of the Sixth Great Lakes Symposium on VLSI. Ames: IEEE, 1996:178-181.

[6] GOLSON S. One-hot state machine design for FPGAs [C]// Proc. 3rdAnnual PLD Design Conference & Exhibit, 1993:1. 1. 3. B.

[7] CHOI H S, CHOI J H, KIM J T. Low-Power AES design using parallel architecture[C]// 2008 International Conference on Convergence & Hybrid Information Technology. Daejeon: IEEE, 2008:413-416.

[8] HESHAM S, ABD EL GHANY M A, HOFMANN K. High throughput architecture for the advanced encryption standard algorithm[C]// 17th International Symposium on Design & Diagnostics of Electronic Circuits & Systems. Warsaw: IEEE, 2014:167-170.

[9] BUI D H, PUSCHINI D, BACLES-MIN S, et al. Ultra low-power and low-energy 32-bit datapath AES architecture for IoT applications[C]// 2016 International Conference on IC Design and Technology (ICICDT). Ho Chi Minh City: IEEE, 2016:1-4.

[10] HAGHIGHIZADEH F, ATTARZADEH H, SHARIFKHANI M. A compact 8-Bit AES crypto-processor [C]// 2010 Second International Conference on Computer & Network Technology. Bangkok: IEEE, 2010:71-75.

作者简介:

李凯利 男,(1993-),硕士研究生. 研究方向为低功耗数字电路设计. E-mail:hi_likaili@163. com.

张卫航 男,(1981-),硕士. 研究方向为低功耗 SoC 设计.

郭桂良 男,(1981-),博士,副研究员. 研究方向为模拟/射频集成电路设计.