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

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

LI Kai-li 1 ， ZHANG Wei-hang 2 ， GUO Gui-liang 1
(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

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.