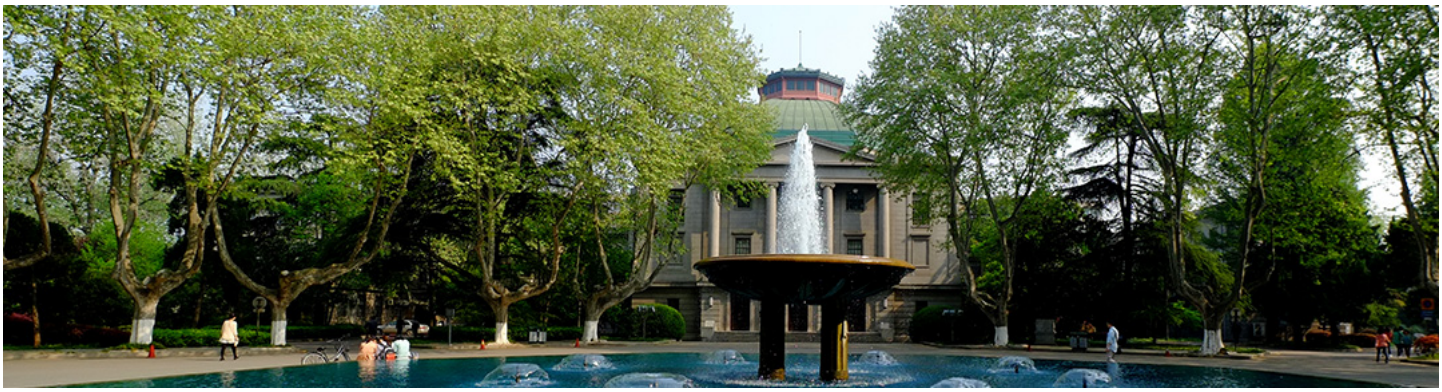

单伟伟、杨军团队在2019 Symposia VLSI Technology and Circuits国际会议发表高能效AES电路成果

发布时间：2019-07-19 浏览次数： 1259

6月9至14日，电子科学与工程学院单伟伟教授、杨军教授等赴日本参加Symposia VLSI Technology and Circuits会议。单伟伟教授在Symposium on VLSI Circuits分会的C20 session作报告，主题为“A 923Gbps/W, 113-Cycle, 2-Sbox Energy-efficient AES Accelerator in 28nm CMOS”。本论文是东南大学在该会议上的重要突破。

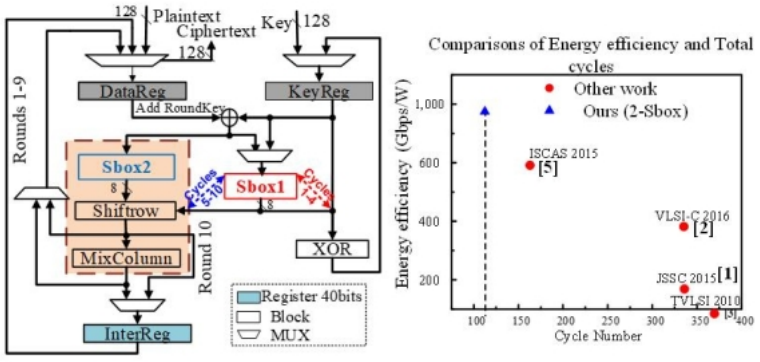

图 1· 双 S 核 AES 电路加密流程图 → → → · 图 2· 能效与同类成果对比图。

论文面向物联网的超低功耗需求和安全需求，设计了超高能效的高级加密算法（Advanced Encryption Standard，AES）加密电路，使其具有小面积和低功耗，满足轻量级应用。论文通过将数据通路从128-bit并行处理变为8-bit串行处理而降低了功耗和面积。同时，针对8-bitAES电路的吞吐率降低的问题，提出了双S核的实现方式，其中1个S核用于数据加密，另一个前4周期用于密钥产生，之后与第一个S核并行用于数据加密，见图1 所示。因此，论文采用11周期实现密钥扩展和数据处理模块，并充分利用二者并行执行的特性，以仅113个周期实现AES加密。

该电路在TSMC 28nm CMOS工艺上完成了流片，测试结果表明，本文的AES电路的能量效率达到了923Gbps/W，是目前最高能效，明显优于比同类研究成果。

VLSI 国际研讨会始于 1987 年，是全球先进半导体与集成电路领域的顶级会议，分为工艺技术（Symposium on VLSI Technology）和电路（Symposium on VLSI Circuits）两大分会。该国际会议每年夏天召开，与每年冬天召开的国际固态电路会议（ISSCC）并称为集成电路领域的两大旗舰会议。（单伟伟）

（责任编辑：杭添 审核：宋业春）

最新更新

东南大学党委召开第三轮巡
东南大学举办“贰零贰零 不
东南大学校长张广军走进课
新 年 献 词
中国第36次南极科学考察队
东南大学20个申报专业全部
东南大学召开2020年度国家
中共东南大学第十四届代表
教育部党组书记、部长陈宝
东南大学举办“第十四届大学

一周热点

东南大学20个申报专业全部
东南大学电磁环境效应研究
东南大学举办“贰零贰零 不
新 年 献 词
东南大学程明教授团队获国
锻造城市空间的“中国名片”
东南大学校长张广军走进课
【新华网】屋盖也可以很“
中国第36次南极科学考察队
中共东南大学第十四届代表