

## 安全技术

### 基于FPGA的16位数据路径的AES IP核

张新贺, 张月华, 刘鸿雁

(辽宁科技大学电子与信息工程学院, 鞍山 114051)

收稿日期 修回日期 网络版发布日期 接受日期

**摘要** 提出一种基于FPGA的16位数据路径的高级加密标准AES IP核设计方案。该方案采用有限状态机实现, 支持密钥扩展、加密和解密。密钥扩展采用非并行密钥扩展, 减少了硬件资源的占用。该方案在Cyclone II FPGA 芯片EP2C35F484上实现, 占用20 070个逻辑单元(少于60%的资源), 系统最高时钟达到100 MHz。与传统的128位数据路径设计相比, 更方便与处理器进行接口。

**关键词** [高级加密标准](#); [IP核](#); [加密](#)

**分类号** [TP309](#)

**DOI:**

通讯作者:

作者个人主页: [张新贺](#); [张月华](#); [刘鸿雁](#)

## 扩展功能

### 本文信息

- ▶ [Supporting info](#)
- ▶ [PDF](#) (124KB)
- ▶ [\[HTML全文\]](#) (0KB)
- ▶ [参考文献\[PDF\]](#)
- ▶ [参考文献](#)

### 服务与反馈

- ▶ [把本文推荐给朋友](#)
- ▶ [加入我的书架](#)
- ▶ [加入引用管理器](#)
- ▶ [引用本文](#)
- ▶ [Email Alert](#)
- ▶ [文章反馈](#)
- ▶ [浏览反馈信息](#)

### 相关信息

- ▶ [本刊中 包含“高级加密标准; IP核; 加密”的 相关文章](#)
- ▶ [本文作者相关文章](#)