通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会



董晓丽,胡予濮,陈杰,李顺波,杨旸.改进的7轮AES-192和8轮AES-256的中间相遇攻击[J].通信学报,2010,(9A):197~201

# 改进的7轮AES-192和8轮AES-256的中间相遇攻击

**DOI：**

**中文关键词：**

**英文关键词：**

**基金项目：**

| 作者 | 单位 |
| --- | --- |
| 董晓丽 | |
| 胡予濮 | |
| 陈杰 | |
| 李顺波 | |
| 杨旸 | |



**中文摘要：**

利用AES密码算法轮变换的特点，构造了一个5轮中间相遇攻击区分器的新变体。基于该区分器变体,使用时空折中方法，针对7轮AES-192和8轮AES-256分别给出了新的攻击方法。研究结果表明，与FSE2008提出的针对AES的中间相遇攻击结果比较，新分析所需的时间复杂度和存储复杂度降低。

**英文摘要：**

查看全文 查看/发表评论 下载PDF阅读器

关闭