

安全技术

高级加密标准Rijndael算法中S盒的替换方案

殷新春^{1,2}, 杨洁¹

(1. 扬州大学计算机科学与工程系, 扬州 225009; 2. 南京大学计算机软件新技术国家重点实验室, 南京 210093)

收稿日期 修回日期 网络版发布日期 2006-10-27 接受日期

摘要 分析了高级加密标准Rijndael算法中非线性变换S盒的设计思想, 对S盒构造过程中的仿射变换加以改变构造出了一批密码性能良好的8'8的S盒, 从方差的角度分析了S盒的雪崩概率, 并从中得到部分规律, 这将有助于寻找更加安全的S盒。

关键词 [高级加密标准](#) [Rijndael](#) [S盒](#) [仿射变换](#)

分类号 [TP309](#)

DOI:

对应的英文版文章: [2006-21-060](#)

通讯作者:

作者个人主页: 殷新春^{1;2}; 杨洁¹

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF \(291KB\)](#)
- ▶ [\[HTML全文\] \(0KB\)](#)
- ▶ [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”的相关文章](#)
- ▶ 本文作者相关文章

- [殷新春](#)
- [杨洁](#)