吉林大学学报(工学版)　2009 39 (01): 137-142　ISSN: 1671-5497 CN: 22-1341/T

单向性策略与AES密钥生成算法的改进

胡亮,袁巍,于孟涛，初剑峰，刘方

吉林大学 计算机科学与技术学院,长春 130012

收稿日期 2008-3-21 修回日期 2008-6-15 网络版发布日期 2009-1-2 接受日期 2008-6-20

摘要　介绍了Mars和AES最终算法Rijndael的密钥生成算法。通过与DES比较，分析了新一代分组密码的密钥生成算法的设计思路。通过研究AES在密钥设计方面存在的不足，提出了一种新的设计策略，并应用该策略对AES的密钥生成算法进行了具体的改进，分析表明这种改进既可以提高原算法安全性，又不牺牲其效率。

关键词　计算机系统结构　单向性　密钥生成　Rijndael　AES

分类号　TP309. 7

One-way property strategy and improvement of key generation algorithm of Rijndael

HU Liang,YUAN Wei,YU Meng-tao, CHU Jian-feng, LIU Fang

College of Computer Science and Technology,Jilin University,Changchun 130012,China

Abstract The key generation algorithm of Rijndael and Mars was introduced. By comparison with Data Encryption Standard (DES), the concept to design new key generation algorithm of block ciphers was analyzed. The weaknesses of the key generation design of Rijndael were investigated, and a new designing strategy was developed, which can be used to improve the key generation algorithm. Analysis shows that such improvement can enhance the safety of the original algorithm without reducing its efficiency.

Key words computer systems organization　one　way property　key generation　Rijndael　AES

DOI:

通讯作者 袁巍 yuanwei1@126.com

扩展功能

本文信息

- Supporting info
- PDF(392KB)
- [HTML全文](0KB)
- 参考文献

服务与反馈

- 把本文推荐给朋友
- 复制索引
- 文章反馈
- 浏览反馈信息

相关信息

- 本刊中 包含“计算机系统结构”的相关文章
- 本文作者相关文章
  - 胡亮
  - 袁巍
  - 于孟涛
  - 初剑峰
  - 刘方