中国计量学院学报
JOURNAL OF CHINA JILIANG UNIVERSITY

◇ 按期浏览
2007 2006
2005

◇ 相关网站链接
万方数据

◇ 相关下载链接
Acrobat Reader
(PDF阅读器)

文章信息

返回上一页检索结果

【文章编号】 1004-1540(2007)01-0054-05

SAFER-64的弱密钥

侯 宇
(中国计量学院 信息工程学院；浙江 杭州 310018)

【摘 要】 通过对SARER-64系统基础模块的深入分析，构建了由6个线性逼近式组成的循环逼近式系统.由于循环性，该逼近式系统可以用来对任意轮次的SARER-64进行多重线性密码分析，从而确定系统的弱密钥.现以五轮SARER-64为例，构建多重线性逼近式并分析系统的弱密钥.

【关键词】 弱密钥；多重线性密码分析；线性逼近式；循环逼近式系统；SAFER-64
【中图分类号】 TP309.7 【文献标识码】 A

Weak keys of SAFER-64

HOU Yu
(Deparement of Computer Science and Technology； China Jiliang University； Hangzhou 310018； China)

Abstract: This paper analyzes the basic modules of SAFER-64 and presents the circulating relations of linear cryptanalysis composed of 6 linear approximations. By the circulating relations, the multiple linear cryptanalysis can be used to determine weak key classes of arbitrate round of SAFER-64. The multiple linear approximations are presented to identify weak key classes of 5 rounds of SAFER-64 in an example.

Key words: weak keys； multiple linear cryptanalysis； linear approximations；

【收稿日期】 2007-01-11
【作者简介】 侯 宇(1958-)，男，浙江温州人，教授.主要研究方向为信息安全理论与技术研究.
【发表于】 2007年第18卷-第1期

文章下载：  阅读器下载： 

此文章所在分类（点选某级分类可查看该分类中的文章列表）：

该文献在中图法分类中的位置:

- 工业技术
  - 自动化技术、计算机技术
    - 计算技术、计算机技术
      - 一般性问题
        - 安全保密
          - 加密与解密

返回上一页检索结果